#3

Attorney Docket No. 1341.1102CIP

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Masashi MITOMO, et al.

Application No.: Group Art Unit:

Filed: February 28, 2002 Examiner:

For: FILTERING APPARATUS, FILTERING METHOD AND COMPUTER PRODUCT

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application Nos. 2001-388444 and 2001-071214

Filed: December 20, 2001 and March 13, 2001, respectively.

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: February 28, 2002 By: _____

James D. Halsey, Jr.
Registration No. 22,729

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

PFJA-01015C-US

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年１２月２０日

出願番号
Application Number: 特願２００１－３８８４４４

[ST.10/C]: [ＪＰ２００１－３８８４４４]

出願人
Applicant(s): 富士通株式会社

CERTIFIED COPY OF PRIORITY DOCUMENT

２００２年 １月１８日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号 出証特２００１－３１１７３５１

【書類名】　特許願

【整理番号】　0152846

【提出日】　平成13年12月20日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 15/00

G06F 13/00

【発明の名称】　フィルタリング装置、フィルタリング方法およびこの方法をコンピュータに実行させるプログラム

【請求項の数】　9

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　三友　仁史

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　鳥居　悟

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　小谷　誠剛

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　滝沢　文恵

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　小野　越夫

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　小谷野　修

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100089118

【弁理士】

【氏名又は名称】　酒井　宏明

【先の出願に基づく優先権主張】

【出願番号】　特願2001- 71214

【出願日】　平成13年 3月13日

【手数料の表示】

【予納台帳番号】　036711

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9717671

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　フィルタリング装置、フィルタリング方法およびこの方法をコンピュータに実行させるプログラム

【特許請求の範囲】

【請求項１】　クライアントと該クライアントからのアクセス要求に応じてサービスを提供するサーバとの間に介在し、前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに受け渡すフィルタリング装置において、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースと、

前記不正パターンデータベースに格納された不正アクセスのパターンおよび所定の見積ルールに基づいて前記アクセス要求の正当性を見積もる見積手段と、

前記見積手段による見積結果および所定の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する判定手段と、

を備えたことを特徴とするフィルタリング装置。

【請求項２】　前記見積手段は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記判定手段は、前記見積手段により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記見積手段により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする請求項１に記載のフィルタリング装置。

【請求項３】　前記見積手段は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、前記判定手段は、前記見積手段により算出された見積値と所定の閾値とを比較して前記アクセス要求を前記サーバに受け渡すか否かを判定することを特徴とする請求項１に記載のフィルタリング装置。

【請求項４】　前記サーバに対する正当アクセスのパターンを格納した正当

パターンデータベースと、前記見積手段による正当性の見積もりの前に、前記アクセス要求が前記正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定する事前判定手段と、をさらに備え、前記見積手段は、前記事前判定手段により正当アクセスのパターンに該当しないものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする請求項１、２または３に記載のフィルタリング装置。

【請求項５】　所定の外部送信ルールに基づいて、前記判定手段により前記サーバに受け渡さないものと判定されたアクセス要求を所定の外部装置に送信する外部送信手段をさらに備えたことを特徴とする請求項１～４のいずれか一つに記載のフィルタリング装置。

【請求項６】　所定の格納ルールに基づいて、前記判定手段により前記サーバに受け渡さないものと判定されたアクセス要求を所定の格納媒体に格納する格納手段をさらに備えたことを特徴とする請求項１～５のいずれか一つに記載のフィルタリング装置。

【請求項７】　所定の更新ルールに基づいて、前記不正パターンデータベース、正当パターンデータベース、見積ルール、判定ルール、外部送信ルール、格納ルールまたは更新ルールを更新する更新手段をさらに備えたことを特徴とする請求項１～６のいずれか一つに記載のフィルタリング装置。

【請求項８】　クライアントからのアクセス要求に応じてサービスを提供するサーバに対し、前記クライアントからのアクセス要求のうちの正当なアクセス要求のみを受け渡すフィルタリング方法において、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースを参照し、該参照した不正アクセスのパターンおよび所定の見積ルールに基づいて前記アクセス要求の正当性を見積もる見積工程と、

前記見積工程による見積結果および所定の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する判定工程と、

を含んだことを特徴とするフィルタリング方法。

【請求項９】　クライアントからのアクセス要求に応じてサービスを提供するサーバに対し、前記クライアントからのアクセス要求のうちの正当なアクセス

要求のみを受け渡すフィルタリング方法をコンピュータに実行させるプログラムにおいて、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースを参照し、該参照した不正アクセスのパターンおよび所定の見積ルールに基づいて前記アクセス要求の正当性を見積もる見積工程と、

前記見積工程による見積結果および所定の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する判定工程と、

をコンピュータに実行させるプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、クライアントと該クライアントからのアクセス要求に応じてサービスを提供するサーバとの間に介在し、前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに受け渡すフィルタリング装置、フィルタリング方法およびこの方法をコンピュータに実行させるプログラムに関する。

【０００２】

近時、ネットワーク技術の進展に伴って、インターネット上の分散システムであるWWW（World Wide Web）の利用が急速に拡大し、クライアントからの各種のリクエスト（アクセス要求）に応じて各種のサービスを提供する各種ＨＴＴＰサーバも累増してきたが、かかるサーバの累増にともなって、クライアントによるサーバへの不正アクセスも増加しつつある。

【０００３】

すなわち、侵入者（イントルーダ）や攻撃者（アタッカ）が企業、団体、個人などのサーバを無権限で不正に利用したり、運用を妨害したり、破壊（クラック）など、サーバを利用する者がその者に与えられた権限により許された行為以外の行為をネットワークを介して意図的におこなうという不正アクセスが増加している。このため、サーバに対する不正アクセスを拒絶することによりサーバの信頼性を確保する必要性が高まりつつある。

【０００４】

【従来の技術】

従来より、クライアントによる不正アクセスからサーバを守るために、インターネットと企業ＬＡＮ（Local Area Network）との間にファイアウォール（Fire Wall）を構築することが一般的におこなわれている。

【０００５】

このファイアウォールは、インターネットに接続したコンピュータやネットワークへの外部からの侵入を防ぐためのソフトウエアであり、企業LANとインターネットの間に、特定のデータやプロトコルだけを通すように設計されたファイアウォール用のコンピュータを置き、LAN内と外部とのデータ交換はすべてこのマシンを通しておこなうことにより、外部からの侵入を防ぐというものである。

【０００６】

また、このファイアウォールに関連して、ネットワークベースあるいはホストベースの不正アクセス検知手法がある。前者のネットワークベースの不正アクセス検知手法は、ネットワークを流れる生のパケットを監視することにより不正アクセスを発見するものであり、後者のホストベースの不正アクセス検知手法は、ホストに蓄えられたログ履歴を監視することにより不正アクセスを発見するものである。

【０００７】

そして、このような不正アクセス検知手法により発見された不正アクセスに基づいて不正アクセスの送信元クライアントを突き止め、この不正アクセスをおこなったクライアントのＩＰアドレスなどの送信元情報をファイアウォール用のコンピュータ内に蓄積することにより、この送信元情報を含んだクライアントからのアクセス要求を不正アクセスとして拒絶することがファイアウォールにおいて一般的におこなわれている。

【０００８】

【発明が解決しようとする課題】

しかしながら、上記の従来技術は、過去に不正アクセスをおこなったクライアントを不正クライアントと認定し、この不正クライアントからのアクセス要求を不正アクセスとして拒絶するものであるため、不正クライアントと認定された後

の不正アクセスに対してはサーバを防御することができるが、不正クライアントと認定されていないクライアントからの不正アクセスに対してはサーバを防御することができないという問題点があった。すなわち、不正クライアントと認定される前の初回の不正アクセスに対してはサーバを防御することができない。

【０００９】

このため、不正クライアントと認定されていないクライアントからの不正アクセスに対していかにサーバを防御するかが極めて重要な課題となっており、望ましくは、アクセス要求の送信元情報を考慮することなく、正当なアクセス要求であるか不正なアクセス要求であるか否かを判定する枠組みが必要とされている。

【００１０】

そこで、この発明は、上述した従来技術による問題点を解消するためになされたものであり、不正クライアントと認定されていないクライアントからの不正アクセスに対してもサーバを防御することができるフィルタリング装置、フィルタリング方法およびこの方法をコンピュータに実行させるプログラムを提供することを目的とする。

【００１１】

【課題を解決するための手段】

上述した課題を解決し、目的を達成するため、請求項１、８または９の発明によれば、図１に示す見積部３２は、Ｗｅｂサーバ４０に対する不正アクセスのパターンを格納した不正リクエストＤＢ（データベース）３３を参照し、不正アクセスのパターンおよび所定の見積ルール３２ａに基づいてクライアント装置１０からのアクセス要求の正当性を見積もり、判定部３４は、見積部３２による見積結果および所定の判定ルール３４ａに基づいてアクセス要求をＷｅｂサーバ４０に受け渡すか否かを判定することとしたので、アクセス要求の送信元情報ではなくアクセス要求の具体的な要求内容に基づいて不正アクセスであるか否かを判定することができる。これにより、正当なアクセス要求のみをＷｅｂサーバ４０に受け渡すことができ、もって不正クライアントと認定されていないクライアント装置１０からの不正アクセスに対してもＷｅｂサーバ４０を防御することができる。

【００１２】

また、請求項２の発明によれば、図１に示す見積部３２は、クライアント装置１０からのアクセス要求が不正リクエストＤＢ３３に格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、クライアント装置１０からのアクセス要求が不正リクエストＤＢ３３に格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、判定部３４は、見積部３２により不正アクセスである旨が見積もられたアクセス要求をＷｅｂサーバ４０に受け渡さないものと判定するとともに、見積部３２により正当アクセスである旨が見積もられたアクセス要求をＷｅｂサーバ４０に受け渡すものと判定することとしたので、アクセス要求が不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを迅速かつ確実に判定することができ、もって不正クライアントと認定されていないクライアント装置１０からの不正アクセスに対しても迅速かつ確実にＷｅｂサーバ４０を防御することができる。

【００１３】

また、請求項３の発明によれば、図１に示す見積部３２は、クライアント装置１０からのアクセス要求が不正リクエストＤＢ３３に格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、判定部３４は、見積部３２により算出された見積値と所定の閾値とを比較してアクセス要求をＷｅｂサーバ４０に受け渡すか否かを判定することとしたので、見積値および閾値の比較によってある程度の幅を持たせて不正アクセスであるか否かを判定することができ、もって不正クライアントと認定されていないクライアント装置１０からの不正アクセスに対してもある程度の幅を持ってＷｅｂサーバ４０を防御することができる。

【００１４】

また、請求項４の発明によれば、図５に示す事前判定部７１は、見積部３２による正当性の見積もりの前に、Ｗｅｂサーバ４０に対する正当アクセスのパターンを格納した正当リクエストＤＢ７２を参照し、クライアント装置１０からのアクセス要求が正当リクエストＤＢ７２に格納された正当アクセスのパターンのい

ずれかに該当するか否かを判定し、見積部３２は、事前判定部７１により正当アクセスのパターンに該当しないものと判定されたアクセス要求のみについて正当性を見積もることとしたので、正当アクセスのパターンと一致するアクセス要求については正当性を見積もることなくＷｅｂサーバ４０に受け渡す一方、正当アクセスのパターンと一致しないアクセス要求のみについて正当性を見積もることができ、もって不正アクセスであるか否かを全体としてより迅速に判定することができる。

【００１５】

また、請求項５の発明によれば、図１に示す外部通報部３７は、所定の通報ルール３７ａに基づいて、判定部３４によりＷｅｂサーバ４０に受け渡さないものと判定されたアクセス要求を所定の外部装置５０に送信することとしたので、不正アクセスに関する情報をＷｅｂサーバ４０の管理者、リクエストフィルタ３０の管理者、サーバ装置２０全体の管理者、ネットワーク全般を監視する公的な機関の管理者などに迅速に通報することができ、もってかかる管理者に対しＷｅｂサーバ４０の保全対策を迅速に促すことができる。

【００１６】

また、請求項６の発明によれば、図１に示すログ管理部３６は、所定の管理ルール３６ａに基づいて、判定部３４によりＷｅｂサーバ４０に受け渡さないものと判定されたアクセス要求を所定の格納媒体３６ｂに格納することとしたので、格納媒体３６ｂに格納された不正アクセスに関する情報を分析することなどができ、もってＷｅｂサーバ４０の更なる保全対策を講じることができる。

【００１７】

また、請求項７の発明によれば、図１に示す更新部３９は、所定の更新ルール３９ａに基づいて、不正リクエストＤＢ３３、正当リクエストＤＢ７２（図５に示す）、見積ルール３２ａ、判定ルール３４ａ、通報ルール３７ａ、管理ルール３６ａまたは更新ルール３９ａを更新することとしたので、新たに発見された不正アクセスのパターンを不正リクエストＤＢ３３に登録することなどができ、もって日々進化する不正アクセスに対して機動的に対応することができる。

【００１８】

【発明の実施の形態】

以下に添付図面を参照して、この発明に係るフィルタリング装置、フィルタリング方法、およびその方法をコンピュータに実行させるプログラムの好適な実施の形態を詳細に説明する。なお、以下に示す実施の形態１～３では、本発明に係るフィルタリング技術を、クライアント装置からのＨＴＴＰ（HyperText Transfer protocol）リクエストに応じてサービスを提供するサーバ装置に適用した場合について説明する。

【００１９】

（実施の形態１）

本実施の形態１では、クライアント装置からのＨＴＴＰリクエストが不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを判定する場合について説明する。

【００２０】

（１）システムの全体構成

まず最初に、本実施の形態１に係るサーバクライアントシステムの構成について説明する。図１は、本実施の形態１に係るサーバクライアントシステムの構成を示すブロック図である。同図に示すように、本実施の形態１に係るサーバクライアントシステムは、Ｗｅｂブラウザ１１をそれぞれ有する複数のクライアント装置１０と、フィルタリング装置としてのリクエストフィルタ３０およびＷｅｂサーバ４０を有するサーバ装置２０とを、インターネットなどのネットワーク１を介して相互に通信可能に接続して構成される。

【００２１】

概略的に、このサーバクライアントシステムにあっては、クライアント装置１０は、Ｗｅｂブラウザ１１によりサーバ装置２０に対してＨＴＴＰリクエストなどの各種の処理要求をおこない、サーバ装置２０のＷｅｂサーバ４０は、クライアント装置１０からのＨＴＴＰリクエストに応じたサービスをクライアント装置１０に提供する。そして、サーバ装置２０のリクエストフィルタ３０は、クライアント装置１０とＷｅｂサーバ４０との間に介在し、クライアント装置１０からのＨＴＴＰリクエストのうちの正当なリクエストのみをＷｅｂサーバ４０に受け

渡す。

【００２２】

ここで、本実施の形態１に係るサーバクライアントシステムは、サーバ装置２０のリクエストフィルタ３０によるフィルタリング処理に特徴があり、具体的には、リクエストフィルタ３０の見積部３２は、クライアント装置１０からのＨＴＴＰリクエストが不正リクエストＤＢ３３に格納された不正アクセスのパターンのいずれかに該当する場合には不正アクセスである旨を見積もり、判定部３４は、見積部３２により不正アクセスである旨が見積もられたＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡さないものと判定することにより、ＨＴＴＰリクエストの送信元情報を問題とすることなく、正当なＨＴＴＰリクエストのみをＷｅｂサーバ４０に受け渡すことができるように構成している。

【００２３】

（２）クライアント装置の構成

次に、図１に示したクライアント装置１０の構成について説明する。同図に示すように、クライアント装置１０は、Ｗｅｂブラウザ１１を備え、基本的には、サーバ装置２０に対してＨＴＴＰリクエストなどの処理要求をおこない、サーバ装置２０のＷｅｂサーバ４０により提供されるＷｅｂデータを解釈して、モニタなどの出力部に表示させる表示制御（ブラウズ処理）をおこなう。

【００２４】

そして、このクライアント装置１０は、悪意を持った使用方法によってサーバ装置２０に対して不正アクセスをおこなうことができる装置でもある。すなわち、クライアント装置１０は、侵入者（イントルーダ）や攻撃者（アタッカ）などの悪意を持ったユーザの使用によっては、Ｗｅｂサーバ４０上のパスワードファイルなどのリモートユーザが見るべきでないファイルを見たり、Ｗｅｂサーバ４０上に存在しないファイルをリクエストしてＷｅｂサーバ４０の機能を停止させたり、コマンド文字列を含んだリクエストによりＷｅｂサーバ４０上で任意のシステムコマンドを実行するなどの不正アクセスをおこない得るものである。このようなクライアント装置１０による不正アクセスに対してＷｅｂサーバ４０を防御するのがリクエストフィルタ３０の役割である。

【００２５】

なお、クライアント装置１０は、たとえば、パーソナルコンピュータやワークステーション、家庭用ゲーム機、インターネットＴＶ、ＰＤＡ(Personal Digital Assistant)、あるいは、携帯電話やＰＨＳ（Personal Handy Phone System）の如き移動体通信端末によって実現することができる。また、クライアント装置１０は、モデム、ＴＡ、ルータなどの通信装置と電話回線を介して、あるいは、専用線を介して、ネットワーク１に接続されており、所定の通信規約（たとえば、ＴＣＰ／ＩＰインターネットプロトコル）に従ってサーバ装置２０にアクセスすることができる。

【００２６】

（３）サーバ装置におけるＷｅｂサーバの構成

次に、図１に示したサーバ装置２０におけるＷｅｂサーバ４０の構成について説明する。同図に示すように、サーバ装置２０のＷｅｂサーバ４０は、リクエストフィルタ３０を介してクライアント装置１０からのＨＴＴＰリクエストを受信し、このＨＴＴＰリクエストに応じてＨＴＭＬ（HyperText Markup Language）などのマークアップ言語により記述された各種の情報を送信するなどのサービスをクライアント装置１０に提供する。

【００２７】

このＷｅｂサーバ４０は、機能概念的には、一般的なＷｅｂサーバと同様の動作をおこなうものであるが、ここでのＷｅｂサーバ４０は、一般的なＷｅｂサーバと異なり、サーバ装置２０においてＨＴＴＰリクエストに割り当てられるポート番号８０のＴＣＰ（Transmission Control Protocol）ポートを監視することはおこなわない。

【００２８】

すなわち、クライアント装置１０からのＨＴＴＰリクエストをＷｅｂサーバ４０により直接に受信するのではなく、リクエストフィルタ３０がＨＴＴＰリクエストを受信し、プロセス間通信をおこなって正当なＨＴＴＰリクエストのみをＷｅｂサーバ４０に受け渡すこととしている。

【００２９】

（４）サーバ装置におけるリクエストフィルタの構成

次に、図１に示したサーバ装置２０におけるリクエストフィルタ３０の構成について説明する。同図に示すように、リクエストフィルタ３０は、受信部３１と、見積部３２と、不正リクエストＤＢ３３と、判定部３４と、送信部３５と、ログ管理部３６と、外部通報部３７と、外部情報取得部３８と、更新部３９とを備える。

【００３０】

このうち、受信部３１は、サーバ装置２０におけるポート番号８０のＴＣＰポートを監視して、クライアント装置１０からのＨＴＴＰリクエストをＷｅｂサーバ４０が受信する前に受信する処理部である。なお、受信部３１によりクライアント装置１０から受信したＨＴＴＰリクエストは、見積部３２および送信部３５に出力される。

【００３１】

見積部３２は、不正リクエストＤＢ３３に格納された不正アクセスのパターンおよび所定の見積ルール３２ａに基づいてＨＴＴＰリクエストの正当性を見積もり、その見積結果を判定部３４に出力する処理部である。

【００３２】

ここで、見積部３２が見積もりに際して参照する不正リクエストＤＢ３３について説明する。図２は、不正リクエストＤＢ３３に格納される情報の構成例を示す図である。同図に示すように、不正リクエストＤＢ３３は、サーバに対する不正アクセスのパターンを格納したデータベースであり、ネットワーク世界で収集された不正アクセスを図示のような形式言語を用いて記述した複数のパターンを記憶している。

【００３３】

例えば、同図に示す「ＵＲＬ＝＜／／」のパターンは、ＵＲＬ（Uniform Resource Locator）の先頭が「／／」である不正リクエストを意味し、「ＣＧＩ＝＝ｐｈｆ、ＡＲＧ＝＜Ｑｎａｍｅ＝ｒｏｏｔ％ＯＡ」のパターンは、ＣＧＩ（Common Gateway Interface）名が「ｐｈｆ」であり、そのある引数の先頭が「Ｑｎａｍｅ＝ｒｏｏｔ％ＯＡ」である不正リクエストを意味し、「ＵＲＬ＜＞．．

¥．．¥．．¥．．」のパターンは、ＵＲＬに「．．¥．．¥．．¥．．」が含まれる不正リクエストを意味し、「ＣＧＩ＞＝．ｈｔｒ」のパターンは、ＣＧＩ名の末尾が「．ｈｔｒ」である不正リクエストを意味する。

【００３４】

なお、図２には示していないが、不正リクエストＤＢ３３には、Ｗｅｂサーバ４０上で任意のシステムコマンドを実行するような不正なコマンド文字列も複数記憶されている。このようなコマンド文字列のパターンを記憶することにより、攻撃方法が既知である不正アクセスだけでなく、攻撃方法が未知である不正アクセスに対してもＷｅｂサーバ４０を防御することができる。

【００３５】

このような不正リクエストＤＢ３３を参照することにより、見積部３２は、所定の見積ルール３２ａに基づいてＨＴＴＰリクエストの正当性の見積もりをおこなう。具体的には、ＨＴＴＰリクエストが不正リクエストＤＢ３３に格納された不正アクセスのパターンのいずれかに該当する場合には、該ＨＴＴＰリクエストは不正アクセスである旨を見積もり、一方、ＨＴＴＰリクエストが不正リクエストＤＢ３３に格納された不正アクセスのパターンのいずれにも該当しない場合には、該ＨＴＴＰリクエストは正当アクセスである旨を見積もる。

【００３６】

図１の説明に戻ると、判定部３４は、見積部３２から受け取った見積結果および所定の判定ルール３４ａに基づいてＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡すか否かを判定し、この判定結果を送信部３５に出力する処理部である。具体的には、見積部３２から不正アクセスである旨の見積結果を受け取った場合には、ＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡さないものと判定し（不可判定）、一方、見積部３２から正当アクセスである旨の見積結果を受け取った場合には、ＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡すものと判定する（可判定）。

【００３７】

送信部３５は、判定部３４から受け取った判定結果に基づいて、受信部３１から受け取ったＨＴＴＰリクエストの送信を制御する処理部である。具体的には、

判定部３４から可判定を受け取った場合には、ＨＴＴＰリクエストをプロセス間通信によりＷｅｂサーバ４０に受け渡す。一方、判定部３４から不可判定を受け取った場合には、ＨＴＴＰリクエストのＷｅｂサーバ４０への受け渡しを拒絶して、この不正リクエストを破棄する。

【００３８】

ログ管理部３６は、所定の管理ルール３６ａに基づいて、判定部３４によりＷｅｂサーバ４０に受け渡さないものと判定された不正リクエストに係る情報を格納媒体３６ｂに格納して管理する処理部である。具体的には、管理ルール３６ａに基づいて、不正リクエストの内容、送信元情報（ＩＰアドレスやホスト名）、送信時刻、見積部３２による見積結果の根拠、判定部３４による判定結果の根拠などの不正リクエストに係る情報を選択的に編集するとともに、この選択編集された情報を不正リクエストの攻撃性の高低などに応じて選択的に格納媒体３６ｂに格納する。例えば、攻撃性の高い不正リクエストのみを格納するなどである。

【００３９】

なお、格納媒体３６ｂに格納された情報は、該格納媒体３６ｂを取り出すことや通信回線を介することなどによりサーバ装置２０の外部に出力することができ、さらに、格納媒体３６ｂに格納された情報を分析して不正アクセスの傾向などを解析することにより、Ｗｅｂサーバ４０の更なる保全のために対策を講じることもできる。

【００４０】

外部通報部３７は、所定の通報ルール３７ａに基づいて、判定部３４によりＷｅｂサーバ４０に受け渡さないものと判定された不正リクエストに係る情報を外部装置５０に通報する処理部である。具体的には、ログ管理部３６による処理と同様、通報ルール３７ａに基づいて、不正リクエストの内容、送信元情報（ＩＰアドレスやホスト名）、送信時刻、見積部３２による見積結果の根拠、判定部３４による判定結果の根拠などの不正リクエストに係る情報を選択的に編集するとともに、この選択編集された情報を不正リクエストの攻撃性の高低などに応じて選択的に外部装置５０に通報する。

【００４１】

この外部通報部３７から通報を受ける外部装置５０は、Ｗｅｂサーバ４０の管理者、リクエストフィルタ３０の管理者、サーバ装置２０全体の管理者、ネットワーク全般を監視する公的な機関（管理センタ）の管理者など（以下、これらを総称して「管理者」という。）が操作する通信装置である。そして、外部通報部３７は、例えば、攻撃性の高い不正リクエストについてはリアルタイムで迅速に管理者に通報し、攻撃性の低い不正リクエストについては非リアルタイムで一括して管理者に通報するなどして、かかる通報を受ける管理者に対してＷｅｂサーバ４０の保全対策を迅速に促すことができる。

【００４２】

外部情報取得部３８は、所定の取得ルール３８ａに基づいて、更新部３９による更新処理に用いられる情報を、外部装置５０やＷｅｂサーバ４０などのリクエストフィルタ３０の外部から能動的または受動的に取得する処理部である。例えば、管理者が外部装置５０を介して入力した新たな不正リクエストのパターンや、管理者が外部装置５０を介して入力した見積ルール３２ａの変更指示情報などを取得するほか、不正リクエストによる被害を受けたＷｅｂサーバ４０から被害の状況や不正アクセスの内容などの情報を取得する。なお、所定の取得ルール３８ａは、権限が認証された管理者からの情報のみを取得するなどの規則である。

【００４３】

更新部３９は、所定の更新ルール３９ａに基づいて、不正リクエストＤＢ３３、見積ルール３２ａ、判定ルール３４ａ、管理ルール３６ａ、通報ルール３７ａ、取得ルール３８ａまたは更新ルール３９ａに格納された情報を更新する処理部である。例えば、外部情報取得部３８から新たな不正リクエストのパターンを受け付けた場合には、この不正リクエストのパターンを不正リクエストＤＢ３３に格納し、また見積ルール３２ａの変更指示情報を受け付けた場合には、この変更指示情報に応じて見積ルール３２ａを変更する。このような更新処理をおこなうことにより、日々進化する不正アクセスに対して機動的に対応することができる。

【００４４】

（５）フィルタリング処理

次に、本実施の形態１によるフィルタリングの処理手順について説明する。図３は、本実施の形態１によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置２０におけるリクエストフィルタ３０の受信部３１は、クライアント装置１０からのＨＴＴＰリクエストをＷｅｂサーバ４０が受信する前に受信する（ステップＳ３０１）。

【００４５】

そして、リクエストフィルタ３０の見積部３２は、不正リクエストＤＢ３３に格納された不正アクセスのパターンおよび所定の見積ルール３２ａに基づいてＨＴＴＰリクエストの正当性を見積もる（ステップＳ３０２）。具体的には、ＨＴＴＰリクエストが不正アクセスのパターンのいずれかに該当する場合には、不正リクエストである旨を見積もり、一方、ＨＴＴＰリクエストが不正アクセスのパターンのいずれにも該当しない場合には、正当リクエストである旨を見積もる。

【００４６】

その後、リクエストフィルタ３０の判定部３４は、見積部３２から受け取った見積結果および所定の判定ルール３４ａに基づいてＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡すか否かを判定する（ステップＳ３０３）。具体的には、見積部３２により正当なリクエストである旨が見積もられたか否かを判定する。

【００４７】

この判定により、正当なリクエストである旨が見積もられたものと判定された場合には（ステップＳ３０３肯定）、リクエストフィルタ３０の送信部３５は、ＨＴＴＰリクエストをプロセス間通信によりＷｅｂサーバ４０に受け渡し（ステップＳ３０４）、Ｗｅｂサーバ４０は、ＨＴＴＰリクエストに応じた情報をクライアント装置１０に送信するなどの正当判定時の処理をおこなう（ステップＳ３０５）。

【００４８】

これとは反対に、不正なリクエストである旨が見積もられたものと判定された場合には（ステップＳ３０３否定）、リクエストフィルタ３０の送信部３５は、ＨＴＴＰリクエストのＷｅｂサーバ４０への受け渡しを拒絶し（ステップＳ３０６）、リクエストフィルタ３０の各部は、不正リクエストの破棄、格納媒体３６

ｂへの格納、外部装置５０への通報などの不正判定時の処理をおこなう（ステップＳ３０７）。

【００４９】

上述してきたように、本実施の形態１によれば、アクセス要求の送信元情報ではなく、アクセス要求の具体的な要求内容が不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを迅速かつ確実に判定することができる。これにより、不正クライアントと認定されていないクライアント装置１０からの不正アクセスに対しても迅速かつ確実にＷｅｂサーバ４０を防御することができる。

【００５０】

（実施の形態２）

ところで、上記実施の形態１では、クライアント装置からのＨＴＴＰリクエストが不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを判定する場合について説明したが、本発明はこれに限定されるものではなく、ＨＴＴＰリクエストが不正アクセスのパターンに該当する度合に応じて不正アクセスであるか否かを判定する場合についても同様に適用することができる。

【００５１】

そこで、本実施の形態２では、ＨＴＴＰリクエストが不正アクセスのパターンに該当する度合に応じて不正アクセスであるか否かを判定する場合について説明する。なお、本実施の形態２においては、サーバクライアントシステムのシステム構成は図１に示すものと同様のものとなるので、ここではその詳細な説明を省略する。

【００５２】

まず最初に、本実施の形態２の特徴部分である見積部３２および判定部３４について説明する。本実施の形態２における見積部３２は、クライアント装置１０からのＨＴＴＰリクエストが不正リクエストＤＢ３３に格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、その見積値を判定部３４に出力する。

【００５３】

具体的には、不正アクセスのパターンから一致するパターンの個数を算出することや、各パターンに危険度数を付与して一致するパターンの危険度数を算出することなどにより、ＨＴＴＰリクエストの危険度を示すＤＩ（Danger　Index）と呼ばれる見積値を算出する。なお、見積値ＤＩは、例えば１～１００の範囲で整数値をとり、危険度が高いＨＴＴＰリクエストほど大きな値が算出されるというものである。

【００５４】

本実施の形態２における判定部３４は、見積部３２により算出された見積値ＤＩと所定の閾値とを比較してＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡すか否かを判定し、この判定結果を送信部３５に出力する。

【００５５】

具体的には、所定の閾値を５０と仮定すると、見積部３２からＤＩが５０以上である見積値を受け取った場合には、ＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡さないものと判定し（不可判定）、一方、見積部３２からＤＩが５０未満である見積値を受け取った場合には、ＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡すものと判定する（可判定）。

【００５６】

次に、本実施の形態２によるフィルタリングの処理手順について説明する。図４は、本実施の形態２によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置２０におけるリクエストフィルタ３０の受信部３１は、クライアント装置１０からのＨＴＴＰリクエストをＷｅｂサーバ４０が受信する前に受信する（ステップＳ４０１）。

【００５７】

そして、リクエストフィルタ３０の見積部３２は、ＨＴＴＰリクエストが不正リクエストＤＢ３３に格納された不正アクセスのパターンに該当する度合に応じて見積値ＤＩを算出する（ステップＳ４０２）。リクエストフィルタ３０の判定部３４は、見積部３２により算出された見積値ＤＩと所定の閾値とを比較してＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡すか否かを判定する（ステップＳ４０３）。具体的には、見積値ＤＩが所定の閾値以上であるか否かを判定する。

【００５８】

この判定により、見積値ＤＩが所定の閾値未満であると判定された場合には（ステップＳ４０３肯定）、リクエストフィルタ３０の送信部３５は、ＨＴＴＰリクエストをプロセス間通信によりＷｅｂサーバ４０に受け渡し（ステップＳ４０４）、Ｗｅｂサーバ４０は、ＨＴＴＰリクエストに応じた情報をクライアント装置１０に送信するなどの正当判定時の処理をおこなう（ステップＳ４０５）。

【００５９】

これとは反対に、見積値ＤＩが所定の閾値以上であると判定された場合には（ステップＳ４０３否定）、リクエストフィルタ３０の送信部３５は、ＨＴＴＰリクエストのＷｅｂサーバ４０への受け渡しを拒絶し（ステップＳ４０６）、リクエストフィルタ３０の各部は、不正リクエストの破棄、格納媒体３６ｂへの格納、外部装置５０への通報などの不正判定時の処理をおこなう（ステップＳ４０７）。

【００６０】

上述してきたように、本実施の形態２によれば、見積値および閾値の比較によってある程度の幅を持たせて不正アクセスであるか否かを判定することができる。これにより、不正クライアントと認定されていないクライアント装置１０からの不正アクセスに対してもある程度の幅を持ってＷｅｂサーバ４０を防御することができる。

【００６１】

（実施の形態３）

ところで、上記実施の形態１および２では、クライアント装置からの全てのＨＴＴＰリクエストについて不正アクセスのパターンに基づく見積もりをおこなう場合について説明したが、本発明にはこれに限定されるものではなく、一部のＨＴＴＰリクエストについてのみ見積もりをおこなう場合についても同様に適用することができる。

【００６２】

そこで、本実施の形態３では、二階層からなるフィルタリング処理をおこない、一部のＨＴＴＰリクエストについてのみ不正アクセスのパターンに基づく見積

もりをおこなう場合について説明する。

【００６３】

図５は、本実施の形態３に係るサーバクライアントシステムの構成を示すブロック図である。なお、図１に示した各部と同様の機能を有する部位には同一符号を付すこととしてその詳細な説明を省略し、本実施の形態３の特徴部分である事前判定部７１および正当リクエストＤＢ７２について説明する。

【００６４】

サーバ装置６０におけるリクエストフィルタ７０の事前判定部７１は、見積部３２による正当性の見積もりの前に、正当リクエストＤＢ７２に格納された正当アクセスのパターンおよび所定の事前判定ルール７１ａに基づいてＨＴＴＰリクエストの見積もりを省くことができるか否かを判定する処理部である。

【００６５】

ここで、事前判定部７１が判定に際して参照する正当リクエストＤＢ７２について説明すると、この正当リクエストＤＢ７２は、Ｗｅｂサーバ４０に対する正当アクセスのパターンを格納したデータベースであり、具体的には、Ｗｅｂサーバ４０上に存在するファイルのうちでリモートユーザに見られても構わないファイルのパスを記憶する。

【００６６】

このリモートユーザに見られても構わないファイルとは、パスワードファイルなどのリモートユーザが見るべきでないファイル以外のファイルであって、例えば、Ｗｅｂサーバ４０に対するＨＴＴＰリクエストのリクエスト内容として非常に高い割合を有する画像ファイルなど、不正アクセスの可能性がほとんどないようなファイルが含まれる。

【００６７】

このような正当リクエストＤＢ７２を参照することにより、事前判定部７１は、所定の事前判定ルール７１ａに基づいてＨＴＴＰリクエストの見積もりを省くことができるか否かを判定する。具体的には、ＨＴＴＰリクエストが正当リクエストＤＢ７２に格納された正当アクセスのパターンのいずれかに該当する場合には、該ＨＴＴＰリクエストの見積もりを省くことができるものと判定し、一方、

ＨＴＴＰリクエストが正当リクエストＤＢ７２に格納された正当アクセスのパターンのいずれにも該当しない場合には、該ＨＴＴＰリクエストの見積もりを省くことができないものと判定する。

【００６８】

そして、事前判定部７１は、見積もりを省くことができないものと判定されたＨＴＴＰリクエストのみを見積部３２に出力し、見積もりを省くことができるものと判定されたＨＴＴＰリクエストについては、見積部３２および判定部３４による処理を省いて、送信部３５を介してＷｅｂサーバ４０に受け渡す。

【００６９】

なお、正当リクエストＤＢ７２に格納される正当アクセスのパターンは、Ｗｅｂサーバ４０に新たな画像ファイルが追加された場合などに応じて、更新部３９により更新される。

【００７０】

次に、本実施の形態３によるフィルタリングの処理手順について説明する。図６は、本実施の形態３によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置６０におけるリクエストフィルタ７０の受信部３１は、クライアント装置１０からのＨＴＴＰリクエストをＷｅｂサーバ４０が受信する前に受信する（ステップＳ６０１）。

【００７１】

そして、リクエストフィルタ７０の事前判定部７１は、正当リクエストＤＢ７２に格納された正当アクセスのパターンおよび所定の事前判定ルール７１ａに基づいてＨＴＴＰリクエストの見積もりを省くことができるか否かを判定する（ステップＳ６０２）。具体的には、ＨＴＴＰリクエストが正当リクエストＤＢ７２に格納された正当アクセスのパターンのいずれかに該当するか否かを判定する。

【００７２】

この判定により、正当アクセスのパターンのいずれかに該当するものと判定された場合には（ステップＳ６０２肯定）、このＨＴＴＰリクエストの正当性の見積もりを省き、リクエストフィルタ７０の送信部３５は、ＨＴＴＰリクエストをプロセス間通信によりＷｅｂサーバ４０に受け渡し（ステップＳ６０５）、Ｗｅ

ｂサーバ４０は、ＨＴＴＰリクエストに応じた情報をクライアント装置１０に送信するなどの正当判定時の処理をおこなう（ステップＳ６０６）。

【００７３】

これとは反対に、正当アクセスのパターンのいずれにも該当しないものと判定された場合には（ステップＳ６０２否定）、このＨＴＴＰリクエストを見積部３２に受け渡し、上記実施の形態１または２によるフィルタリング処理と同様の処理をおこなう（ステップＳ６０３～６０８）。

【００７４】

すなわち、リクエストフィルタ７０の見積部３２は、ＨＴＴＰリクエストの正当性を見積もり（ステップＳ６０３）、判定部３４は、ＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡すか否かを判定する（ステップＳ６０４）。

【００７５】

この判定により、正当なリクエストである旨が見積もられたものと判定された場合には（ステップＳ６０４肯定）、リクエストフィルタ７０の送信部３５は、ＨＴＴＰリクエストをプロセス間通信によりＷｅｂサーバ４０に受け渡し（ステップＳ６０５）、Ｗｅｂサーバ４０は、ＨＴＴＰリクエストに応じた情報をクライアント装置１０に送信するなどの正当判定時の処理をおこなう（ステップＳ６０６）。

【００７６】

これとは反対に、不正なリクエストである旨が見積もられたものと判定された場合には（ステップＳ６０４否定）、リクエストフィルタ７０の送信部３５は、ＨＴＴＰリクエストのＷｅｂサーバ４０への受け渡しを拒絶し（ステップＳ６０７）、リクエストフィルタ７０の各部は、不正リクエストの破棄、格納媒体３６ｂへの格納、外部装置５０への通報などの不正判定時の処理をおこなう（ステップＳ６０８）。

【００７７】

上述してきたように、本実施の形態３によれば、画像ファイルを要求するＨＴＴＰリクエストのような要求の割合は高いが攻撃性は極めて低いものについては、見積部３２および判定部３４による処理を省いて迅速な処理をおこなうことが

できるとともに、パスワードファイルやＷｅｂサーバ４０上に存在しないファイルを要求するＨＴＴＰリクエストのような攻撃性が高いものについては、見積部３２および判定部３４による処理をおこなって、かかる攻撃を有効に防御することができる。

【００７８】

なお、本実施の形態１～３では、クライアント装置１０からのＨＴＴＰリクエストをフィルタリングする場合について説明したが、本発明はこれに限定されるものではなく、ＦＴＰ（File Transfer Protocol）、ｔｅｌｎｅｔ、コンソールなど、クライアント装置１０からＷｅｂサーバ４０に入力されるあらゆる情報をフィルタリングする場合に同様に適用することができる。

【００７９】

また、本実施の形態１～３では、フィルタリング装置としてのリクエストフィルタ３０、７０をサーバ装置２０、６０に設けた場合について説明したが、本発明はこれに限定されるものではなく、例えば、それぞれのクライアント装置側にリクエストフィルタを設けたり、一つのリクエストフィルタにより複数のＷｅｂサーバを防御するなど、クライアント装置とＷｅｂサーバとの間にリクエストフィルタが介在するあらゆるシステム構成において同様に適用することができる。

【００８０】

なお、本実施の形態１～３で説明したフィルタリング方法は、あらかじめ用意されたプログラムをパーソナル・コンピュータやワークステーションなどのコンピュータで実行することによって実現することができる。このプログラムは、インターネットなどのネットワークを介して配布することができる。また、このプログラムは、ハードディスク、フレキシブルディスク（ＦＤ）、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行することもできる。

【００８１】

（実施の形態４）

ところで、上記実施の形態１～３では、サーバに対する不正アクセスのパターンを格納した不正リクエストＤＢ３３を参照することによって、アクセス要求の

要求内容から不正アクセスと把握できるアクセス要求を破棄する場合を説明したが、本発明はこれに限定されるものではなく、サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求を破棄する場合についても同様に適用することができる。

【００８２】

すなわち、サーバに対する不正アクセスとしては、アクセス要求の要求内容から不正アクセスと把握されるアクセス要求の他に、アクセス要求の要求内容からは正当アクセスと把握されるが、サーバに対するアクセス要求の統計からみて不正アクセスとみなされるべきアクセス要求がある。例えば、特定のクライアント装置１０からのアクセス要求を集中的に受信している場合や、特定の要求内容からなるアクセス要求を集中的に受信している場合には、個々の要求内容からは正当アクセスと把握されたしても、アクセス要求の統計からはサーバダウンを狙ったものと考えられるので、不正アクセスとみなされるべきである。

【００８３】

そこで、本実施の形態４では、サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求に関する情報を格納したデータベースをも参照して正当性を見積もることによって、サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求を破棄するフィルタリング処理も実行することができるようにしている。以下、本実施の形態４に係るサーバクライアントシステムにおけるサーバ装置の構成と、本実施の形態４によるフィルタリングの処理手順とを説明する。

【００８４】

（１）サーバ装置の構成

まず最初に、本実施の形態４に係るサーバクライアントシステムにおけるサーバ装置の構成を説明する。図７は、本実施の形態４に係るサーバクライアントシステムの構成を示すブロック図である。同図に示すように、本実施の形態４におけるサーバ装置８０は、Ｗｅｂサーバ４０と、リクエストフィルタ８１とを備え、さらに、このリクエストフィルタ８１は、受信部３１と、第１見積部８２と、不正リクエストＤＢ８３と、第１判定部８４と、第２見積部８５と、統計的不正

リクエストＤＢ８６と、第２判定部８７と、送信部８８とを備える。

【００８５】

このうち、Ｗｅｂサーバ４０および受信部３１は、図１に示した同一符号を付している各部と同様の機能を有する。また、第１見積部８２、不正リクエストＤＢ８３および第１判定部８４は、図１に示した見積部３２、不正リクエストＤＢ３３および判定部３４と同様の機能をそれぞれ有し、上記実施の形態１または２に示したフィルタリング処理と同様の処理、すなわち、ＨＴＴＰリクエストの要求内容から不正リクエストと把握できるＨＴＴＰリクエストを破棄するフィルタリング処理（パターンに基づくフィルタリング処理）を実行するものである。

【００８６】

すなわち、不正リクエストＤＢ８３は、サーバに対する不正アクセスのパターンを格納したデータベースである。また、第１見積部８２は、不正リクエストＤＢ８３に格納された不正アクセスのパターンおよび所定の見積ルール８２ａに基づいてＨＴＴＰリクエストの正当性を見積もり、その見積結果（正当リクエスト若しくは不正リクエストである旨の見積結果、または見積値ＤＩ）を第１判定部８４に出力する。

【００８７】

さらに、第１判定部８４は、第１見積部８２から受け取った見積結果および所定の判定ルール８４ａに基づいてＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡すか否か（すなわち、正当リクエストである旨が見積もられたか否か、または見積値ＤＩが所定の閾値以下であるか否か）を判定し、この判定結果を送信部８８に出力するか、またはＨＴＴＰリクエストを第２見積部８５に出力する。

【００８８】

これらによって、ＨＴＴＰリクエストの要求内容から不正リクエストと把握されたＨＴＴＰリクエスト（すなわち、不正リクエストである旨が見積もられたＨＴＴＰリクエスト、または見積値ＤＩが所定の閾値以下でなかったＨＴＴＰリクエスト）については、ＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡さないものと判定され、不可判定が送信部８８に出力されることとなる。

【００８９】

一方、これらによって、ＨＴＴＰリクエストの要求内容から不正リクエストと把握されなかったＨＴＴＰリクエスト（すなわち、正当リクエストである旨が見積もられたＨＴＴＰリクエスト、または見積値ＤＩが所定の閾値以下であったＨＴＴＰリクエスト）については、Ｗｅｂサーバ４０に対するＨＴＴＰリクエストの統計からみて不正リクエストとみなされるＨＴＴＰリクエストを破棄するフィルタリング処理（統計に基づくフィルタリング処理）を実行するために、第２見積部８５に出力されることとなる。

【００９０】

第２見積部８５は、統計的不正リクエストＤＢ８６に格納された統計的情報および所定の見積ルール８５ａに基づいてＨＴＴＰリクエストの正当性を見積もり、その見積結果を第２判定部８７に出力する処理部である。

【００９１】

ここで、上記の統計的不正リクエストＤＢ８６は、サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求に関する情報を格納したデータベースである。具体的には、Ｗｅｂサーバ４０に対してＨＴＴＰリクエストを送信したクライアント装置１０のうち、所定時間内のリクエスト数が所定数を超えたクライアント装置１０の送信元情報（ＩＰアドレス）や、Ｗｅｂサーバ４０に対して送信されたＨＴＴＰリクエストの要求内容のうち、所定時間内のリクエスト数が所定数を超えた要求内容を格納する。

【００９２】

このような送信元情報や要求内容を格納することとしたのは、特定のクライアント装置１０からのＨＴＴＰリクエストを短時間で集中的に受信しているような場合や、特定の要求内容のＨＴＴＰリクエストを短時間で集中的に受信しているような場合には、サーバダウンを狙った不正リクエストとみなすことができるからである。

【００９３】

そして、第２見積部８５は、このような情報を格納した統計的不正リクエストＤＢ８６を参照することにより、所定の見積ルール８５ａに基づいてＨＴＴＰリクエストの正当性の見積もりをおこなう。具体的には、ＨＴＴＰリクエストの送

信元情報が統計的不正リクエストＤＢ８６に格納された送信元情報のいずれかに該当する場合、またはＨＴＴＰリクエストの要求内容が統計的不正リクエストＤＢ８６に格納された要求内容のいずれかに該当する場合には、該ＨＴＴＰリクエストは不正リクエストである旨を見積もる。

【００９４】

一方、ＨＴＴＰリクエストの送信元情報が統計的不正リクエストＤＢ８６に格納された送信元情報のいずれにも該当しない場合、およびＨＴＴＰリクエストの要求内容が統計的不正リクエストＤＢ８６に格納された要求内容のいずれかにも該当しない場合には、第２見積部８５は、該ＨＴＴＰリクエストは正当リクエストである旨を見積もる。

【００９５】

第２判定部８７は、第２見積部８５から受け取った見積結果および所定の判定ルール８７ａに基づいてＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡すか否かを判定し、この判定結果を送信部８８に出力する処理部である。具体的には、第２見積部８５から不正リクエストである旨の見積結果を受け取った場合には、ＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡さないものと判定する（不可判定）。一方、第２見積部８５から正当リクエストである旨の見積結果を受け取った場合には、ＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡すものと判定する（可判定）。

【００９６】

送信部８８は、第１判定部８４および／または第２判定部８７から受け取った判定結果に基づいて、受信部３１から受け取ったＨＴＴＰリクエストの送信を制御するアクセス要求受渡手段である。具体的には、第２判定部８７から可判定を受け取った場合には、ＨＴＴＰリクエストをプロセス間通信によりＷｅｂサーバ４０に受け渡す。一方、第１判定部８４または第２判定部８７から不可判定を受け取った場合には、ＨＴＴＰリクエストのＷｅｂサーバ４０への受け渡しを拒絶して、この不正リクエストを破棄する。

【００９７】

すなわち、送信部８８は、第１判定部８４および第２判定部８７によりＷｅｂ

サーバ４０に受け渡すものと判定されたＨＴＴＰリクエスト（すなわち、ＨＴＴＰリクエストの要求内容から不正リクエストと把握されず、かつ、Ｗｅｂサーバ４０に対するＨＴＴＰリクエストの統計からみて不正リクエストとみなされなかったＨＴＴＰリクエスト）のみを、正当なＨＴＴＰリクエストとしてＷｅｂサーバ４０に受け渡す。

【００９８】

なお、図７には図示していないが、本実施の形態４のリクエストフィルタ８１は、図１に示した実施の形態１のリクエストフィルタ３０と同様、ログ管理部、外部通信部、外部情報取得部および更新部を備えるものである。すなわち、本実施の形態４のリクエストフィルタ８１においては、実施の形態１のリクエストフィルタ３０と同様、ログ管理部は、所定の格納ルールに基づいて、送信部８８によりＷｅｂサーバ４０に受け渡されなかったＨＴＴＰリクエストに係る情報を所定の格納媒体に格納して管理する。

【００９９】

また、外部通信部は、所定の通報ルールに基づいて、送信部８８によりＷｅｂサーバ４０に受け渡されなかったＨＴＴＰリクエストに係る情報を外部装置に通報する。さらに、外部情報取得部は、所定の取得ルールに基づいて、更新部による更新処理に用いられる情報を、外部装置やＷｅｂサーバ４０などのリクエストフィルタ８１の外部から能動的または受動的に取得する。

【０１００】

そして、更新部は、所定の更新ルールに基づいて、不正リクエストＤＢ３３、見積ルール３２ａ、判定ルール３４ａ、見積ルール８５ａ、判定ルール８７ａ、管理ルール、通報ルール、取得ルールまたは更新ルールに格納された情報を更新するとともに、所定の更新ルールおよびＷｅｂサーバ４０に対するアクセス要求の統計に基づいて、統計的不正リクエストＤＢ８６に格納された情報も更新する。

【０１０１】

（２）フィルタリング処理

次に、本実施の形態４によるフィルタリングの処理手順について説明する。図

８は、本実施の形態４によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置８０におけるリクエストフィルタ８１の受信部３１は、クライアント装置１０からのＨＴＴＰリクエストをＷｅｂサーバ４０が受信する前に受信する（ステップＳ８０１）。

【０１０２】

続いて、リクエストフィルタ８１は、このＨＴＴＰリクエストを第１見積部８２に受け渡し、上記実施の形態１または２によるフィルタリング処理と同様の処理、すなわち、パターンに基づくフィルタリング処理を実行する（ステップＳ８０２、Ｓ８０３、Ｓ８０８およびＳ８０９）。

【０１０３】

すなわち、第１見積部８２は、不正リクエストＤＢ８３に格納されたサーバに対する不正アクセスのパターンに基づいて、ＨＴＴＰリクエストの正当性を見積もり（ステップＳ８０２）、第１判定部８４は、ＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡すか否か（すなわち、正当リクエストである旨が見積もられたか否か、または見積値ＤＩが所定の閾値以下であるか否か）を判定する（ステップＳ８０３）。

【０１０４】

この判定により、ＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡さないものと判定された場合（すなわち、不正リクエストである旨が見積もられた場合、または見積値ＤＩが所定の閾値以上である場合）には（ステップＳ８０３否定）、送信部８８は、ＨＴＴＰリクエストのＷｅｂサーバ４０への受け渡しを拒絶する（ステップＳ８０８）。さらに、リクエストフィルタ８１の各部は、不正リクエストの破棄、格納媒体への格納、外部装置への通報などの不正判定時の処理をおこなう（ステップＳ８０９）。

【０１０５】

これとは反対に、ＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡すものと判定された場合（すなわち、正当リクエストである旨が見積もられた場合、または見積値ＤＩが所定の閾値以下である場合）には（ステップＳ８０３肯定）、ＨＴＴＰリクエストは、統計に基づくフィルタリング処理を実行するために、第２見

積部８５に出力される。そして、第２見積部８５は、統計的不正リクエストＤＢ８６に格納された統計的情報および所定の見積ルール８５ａに基づいてＨＴＴＰリクエストの正当性を見積もる（ステップＳ８０４）。

【０１０６】

具体的には、第２見積部８５は、ＨＴＴＰリクエストの送信元情報が統計的不正リクエストＤＢ８６に格納された送信元情報のいずれかに該当する場合、またはＨＴＴＰリクエストの要求内容が統計的不正リクエストＤＢ８６に格納された要求内容のいずれかに該当する場合には、該ＨＴＴＰリクエストは不正リクエストである旨を見積もる。一方、ＨＴＴＰリクエストの送信元情報が統計的不正リクエストＤＢ８６に格納された送信元情報のいずれにも該当しない場合、およびＨＴＴＰリクエストの要求内容が統計的不正リクエストＤＢ８６に格納された要求内容のいずれかにも該当しない場合には、第２見積部８５は、該ＨＴＴＰリクエストは正当リクエストである旨を見積もる。

【０１０７】

その後、第２判定部８７は、第２見積部８５から受け取った見積結果および所定の判定ルール８７ａに基づいてＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡すか否か、すなわち正当リクエストである旨が見積もられたか否かを判定する（ステップＳ８０５）。

【０１０８】

この判定により、正当リクエストである旨が見積もられた場合には（ステップＳ８０５肯定）、送信部８８は、ＨＴＴＰリクエストをプロセス間通信によりＷｅｂサーバ４０に受け渡し（ステップＳ８０６）、Ｗｅｂサーバ４０は、ＨＴＴＰリクエストに応じた情報をクライアント装置１０に送信するなどの正当判定時の処理をおこなう（ステップＳ８０７）。

【０１０９】

これとは反対に、不正リクエストである旨が見積もられた場合には（ステップＳ８０５否定）、送信部８８は、ＨＴＴＰリクエストのＷｅｂサーバ４０への受け渡しを拒絶し（ステップＳ８０８）、リクエストフィルタ８１の各部は、不正リクエストの破棄、格納媒体への格納、外部装置への通報などの不正判定時の処

理をおこなう（ステップＳ８０９）。

【０１１０】

上記した一連の処理によって、ＨＴＴＰリクエストの要求内容から不正リクエストと把握されず、かつ、Ｗｅｂサーバ４０に対するＨＴＴＰリクエストの統計からみて不正リクエストとみなされなかったＨＴＴＰリクエストのみが、正当なＨＴＴＰリクエストとしてＷｅｂサーバ４０に受け渡されることとなる。

【０１１１】

上述してきたように、本実施の形態４によれば、サーバに対する不正アクセスのパターンを格納した不正リクエストＤＢ８３を参照して正当性を見積もるとともに、サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求に関する情報を格納した統計的不正リクエストＤＢ８６をも参照して正当性を見積もることとしたので、アクセス要求の要求内容から不正アクセスと把握されるアクセス要求のみならず、サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求をも破棄することができる。これによって、クライアント装置１０による不正アクセスからＷｅｂサーバ４０を一層確実に防御することができる。

【０１１２】

（３）本実施の形態４の変形例

さて、これまで本実施の形態４について説明したが、本発明は上述した実施の形態４以外にも、上記特許請求の範囲に記載した技術的思想の範囲内において種々の異なる実施の形態にて実施されてもよいものである。

【０１１３】

例えば、本実施の形態４では、統計的不正リクエストＤＢ８６が所定の送信元情報および要求内容を格納する場合を説明したが、本発明はこれに限定されるものではなく、統計的不正リクエストＤＢ８６が所定の送信元情報または要求内容のいずれか一方を格納する場合にも同様に適用することができる。

【０１１４】

すなわち、統計的不正リクエストＤＢ８６が所定の送信元情報のみを記憶する場合には、第２見積部８５は、ＨＴＴＰリクエストの送信元情報が統計的不正リ

クエストＤＢ８６に格納された送信元情報のいずれかに該当することを条件に該アクセス要求は不正アクセスである旨を見積もるとともに、いずれにも該当しないことを条件に該アクセス要求は正当アクセスである旨を見積もることとなる。

【０１１５】

一方、統計的不正リクエストＤＢ８６が所定の要求内容のみを記憶する場合には、第２見積部８５は、ＨＴＴＰリクエストの要求内容が統計的不正リクエストＤＢ８６に格納された要求内容のいずれかに該当することを条件に該アクセス要求は不正アクセスである旨を見積もるとともに、いずれにも該当しないことを条件に該アクセス要求は正当アクセスである旨を見積もることとなる。

【０１１６】

また、本実施の形態４では、ＨＴＴＰリクエストの送信元情報や要求内容が、統計的不正リクエストＤＢ８６に格納された所定の送信元情報や要求内容に該当するか否かによって不正アクセスであるか否かを判定する場合について説明したが、本発明はこれに限定されるものではなく、統計的不正リクエストＤＢ８６に格納された所定の送信元情報や要求内容に該当する度合に応じて不正アクセスであるか否かを判定する場合にも同様に適用することができる。

【０１１７】

すなわち、この場合には、上記実施の形態２と同様、統計的不正リクエストＤＢ８６に格納された所定の送信元情報や要求内容にそれぞれ危険度数を付与しておき、第２見積部８５は、ＨＴＴＰリクエストの送信元情報や要求内容に対応する危険度数を用いて、ＨＴＴＰリクエストの危険度を示すＤＩ（Danger　Index）と呼ばれる見積値を算出し、第２判定部８７は、この算出された見積値ＤＩと所定の閾値とを比較して不正アクセスであるか否かを判定することとなる。

【０１１８】

また、本実施の形態４では、第２見積部８５が、第１判定部８４によりＷｅｂサーバ４０に受け渡すものと判定されたＨＴＴＰリクエストのみについて正当性を見積もる場合、すなわち、パターンに基づくフィルタリング処理を実行した後に、統計に基づくフィルタリング処理を実行する場合を説明したが、本発明はこれに限定されるものではない。

【０１１９】

例えば、第１見積部８２が、第２判定部８７によりＷｅｂサーバ４０に受け渡すものと判定されたＨＴＴＰリクエストのみについて正当性を見積もる場合にも同様に適用することができる。この場合には、統計に基づくフィルタリング処理を実行した後に、パターンに基づくフィルタリング処理を実行することとなる。

【０１２０】

また、例えば、上記実施の形態３で説明した事前判定処理を追加し、事前判定部が、第２判定部８７によりＷｅｂサーバ４０に受け渡すものと判定されたアクセス要求のみについて事前判定処理をおこなう場合にも同様に適用することができる。この場合には、統計に基づくフィルタリング処理を実行した後に、事前判定処理がおこなわれ、この事前判定処理に続いて、パターンに基づくフィルタリング処理を実行することとなる。

【０１２１】

なお、事前判定処理を追加する場合には、統計に基づくフィルタリング処理よりも後に事前判定処理をおこなう必要がある。この統計に基づくフィルタリング処理よりも前に事前判定処理をおこなうと、上記のようなＨＴＴＰリクエストが正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するものと判定されてしまい、統計に基づくフィルタリング処理によって破棄されることなく、Ｗｅｂサーバ４０に受け渡されるおそれが生じるからである。

【０１２２】

さらに、本発明は、パターンに基づくフィルタリング処理や統計に基づくフィルタリング処理を階層的に実行する場合に限定されず、これらの各処理を並列的に実行する場合にも同様に適用することができる。すなわち、この場合には、図９に示すように、サーバ装置９０のリクエストフィルタ９１は、受信部３１と送信部８８との間に、パターンに基づくフィルタリング処理を実行する第１見積部８２および第１判定部８４と、統計に基づくフィルタリング処理を実行する第２見積部８５および第２判定部８７とを、並列的に備えることとなる。このようなリクエストフィルタ９１を構成することにより、不正アクセスであるか否かを一層迅速に判定することが可能になる。

【０１２３】

（実施の形態５）

ところで、上記実施の形態４では、統計的不正リクエストＤＢ８６を参照して統計に基づくフィルタリング処理を実行する場合を説明したが、本発明は、この統計的不正リクエストＤＢ８６に格納された情報を動的に更新しながら、フィルタリング処理を実行することもできる。

【０１２４】

すなわち、実施の形態４では、第２見積部８５は、ＨＴＴＰリクエストの送信元情報が統計的不正リクエストＤＢ８６に格納された送信元情報のいずれかに該当する場合、またはＨＴＴＰリクエストの要求内容が統計的不正リクエストＤＢ８６に格納された要求内容のいずれかに該当する場合には、該ＨＴＴＰリクエストは不正リクエストである旨を見積もることとしている。

【０１２５】

しかしながら、特定のクライアント装置１０（送信元情報）からのＨＴＴＰリクエストや特定の要求内容のＨＴＴＰリクエストの受信が急激に増加しているような状況において、この特定の送信元情報や要求内容が統計的不正リクエストＤＢ８６にリアルタイムで追加されなかったのでは、サーバに対するＨＴＴＰリクエストの統計からみて不正リクエストとみなされるＨＴＴＰリクエストがＷｅｂサーバ４０に送信されてしまう。

【０１２６】

その一方で、統計的不正リクエストＤＢ８６に格納された特定の送信元情報や要求内容のＨＴＴＰリクエストの受信が減少しているような状況において、この特定の送信元情報や要求内容が統計的不正リクエストＤＢ８６からリアルタイムで削除されなかったのでは、サーバに対するＨＴＴＰリクエストの統計からみて不正リクエストとはみなされないＨＴＴＰリクエストまでが破棄されてしまう。

【０１２７】

そこで、本実施の形態５では、統計的不正リクエストＤＢ８６に格納された情報を動的に更新することによって、サーバに対するＨＴＴＰリクエストの統計からみて不正リクエストとみなされるＨＴＴＰリクエストを精度良く確実に破棄す

ることができるようにしている。以下、本実施の形態５に係るサーバクライアントシステムにおけるサーバ装置の構成を説明する。

【０１２８】

図１０は、本実施の形態５に係るサーバクライアントシステムの構成を示すブロック図である。なお、図１または図７に示した各部と同様の機能を有する部位には同一符号を付すこととしてその詳細な説明を省略し、本実施の形態５の特徴部分であるアクセス管理部１０２および動的更新部１０３について説明する。

【０１２９】

サーバ装置１００におけるリクエストフィルタ１０１のアクセス管理部１０２は、サーバ装置１００に対して送信されたＨＴＴＰリクエストの送信元情報、要求内容および送信時刻を履歴として管理するメモリである。

【０１３０】

そして、動的更新部１０３は、アクセス管理部１０２により管理される情報および所定の更新ルール１０３ａに基づいて、統計的不正リクエストＤＢ８６に格納された情報を動的に更新する処理部である。具体的には、アクセス管理部１０２を参照し、特定のクライアント装置１０からＷｅｂサーバ４０に対して送信された所定時間内のＨＴＴＰリクエスト数が所定の上限数を超えた場合には、この送信元情報を統計的不正リクエストＤＢ８６に追加する。

【０１３１】

その一方で、動的更新部１０３は、統計的不正リクエストＤＢ８６に格納された送信元情報のクライアント装置１０からＷｅｂサーバ４０に対して送信された所定時間内のＨＴＴＰリクエスト数が所定の下限数を下回った場合には、この送信元情報を統計的不正リクエストＤＢ８６から削除する。

【０１３２】

さらに、動的更新部１０３は、アクセス管理部１０２を参照し、Ｗｅｂサーバ４０に対して送信された特定のＨＴＴＰリクエストのリクエスト数が所定時間内に所定の上限数を超えた場合には、このＨＴＴＰリクエストの要求内容を統計的不正リクエストＤＢ８６に追加する一方、統計的不正リクエストＤＢ８６に格納された要求内容のＨＴＴＰリクエストのリクエスト数が所定時間内に所定の下限

数を下回った場合には、この要求内容を統計的不正リクエストＤＢ８６から削除する。

【０１３３】

なお、上記した「所定の上限数」は、これを超えた場合にはサーバダウンを狙った不正アクセスとみなれるべきという閾値であり、一方、上記した「所定の下限数」は、これを下回った場合にはサーバダウンを狙った不正アクセスとみなれるべきでないという閾値である。そして、これらの上限数および下限数は、Ｗｅｂサーバ４０の処理能力などを考慮して設定される。

【０１３４】

上述してきたように、本実施の形態５によれば、所定時間内にＷｅｂサーバ４０に対してＨＴＴＰリクエストを送信した各クライアント装置１０ごとのリクエスト数や、所定時間内にＷｅｂサーバ４０に対して送信されたＨＴＴＰリクエストの各要求内容ごとのリクエスト数に応じて、統計的不正リクエストＤＢ８６に格納される送信元情報や要求内容を追加したり削除することとしたので、Ｗｅｂサーバ４０に対するＨＴＴＰリクエストの統計からみて不正リクエストとみなされるＨＴＴＰリクエストを精度良く確実に破棄することができる。

【０１３５】

なお、本実施の形態５では、統計的不正リクエストＤＢ８６に格納される送信元情報および要求内容をともに更新する場合を説明したが、本発明はこれに限定されるものではなく、統計的不正リクエストＤＢ８６に送信元情報または要求内容のいずれか一方を格納する場合には、格納される送信元情報または要求内容のみを追加したり削除するなど、統計的不正リクエストＤＢ８６に格納される情報に応じて更新することができる。

【０１３６】

また、本実施の形態５では、アクセス管理部１０２のみを参照して、統計的不正リクエストＤＢ８６を動的に更新する場合を説明したが、本発明はこれに限定されるものではなく、例えば、ログ管理部３６およびアクセス管理部１０２の両者を参照して、統計的不正リクエストＤＢ８６を動的に更新する場合にも同様に適用することができる。

【０１３７】

すなわち、ログ管理部３６に追加された送信元情報を統計的不正リクエストＤＢ８６にも追加したり、また、ログ管理部３６に格納されている送信元情報については、統計的不正リクエストＤＢ８６において高度の危険度数を付与したり、さらに、リクエスト数が所定の下限値を下回った場合でも、統計的不正リクエストＤＢ８６から削除しないなど、ログ管理部３６をも参照して統計的不正リクエストＤＢ８６を動的に更新することができる。

【０１３８】

（実施の形態６）

ところで、上記実施の形態１～５では、クライアント装置１０から送信されたＨＴＴＰリクエストに対して種々の見積もりをおこなって不正アクセスを破棄する場合を説明したが、本発明はこれに限定されるものではなく、ＨＴＴＰリクエストに応じてＷｅｂサーバ４０からクライアント装置１０に送信されるレスポンスに対しても、その正当性を見積もって不正なレスポンスを破棄することもできる。

【０１３９】

すなわち、上記実施の形態１～５では、不正リクエストのパターンを不正リクエストＤＢ３３などに格納し、クライアント装置１０からのＨＴＴＰリクエストが不正リクエストのパターンに一致するか否かなどによって不正アクセスであるか否かを判定したが、不正リクエストのなかには、パターンとして記述し難い不正リクエストもある。例えば、Ｗｅｂサーバ４０が所有しないファイルを要求するＨＴＴＰリクエストを送信することによって、ディレクトリ情報など、Ｗｅｂサーバ４０の外部に漏れてはいけない秘匿情報をレスポンスとして受信しようとする不正アクセスなどである。

【０１４０】

このような不正アクセスは、Ｗｅｂサーバ４０が所有しないファイルを要求するものであるところ、パターンとして記述し難いため、不正リクエストのパターンに一致するか否かなどを見積もるだけでは、これを不正アクセスと判定することができない。一方、このような不正アクセスに応じてＷｅｂサーバ４０からク

ライアント装置１０に送信されるレスポンスには、ディレクトリ情報など、Ｗｅｂサーバ４０の外部に漏れてはいけない秘匿情報が含まれるので、このような秘匿情報がレスポンスに含まれるか否かを見積もれば、パターンとして記述し難い不正アクセスに対しても対応することができると考えられる。

【０１４１】

そこで、本実施の形態６では、クライアント装置１０に対して送信されるべきでない不正レスポンスのパターンを格納したデータベースを参照して、レスポンスの正当性を見積もることによって、パターンとして記述し難い不正アクセスに応じてクライアント装置１０に送信されようとする不正なレスポンスをも破棄することができるようにしている。以下、本実施の形態６に係るサーバクライアントシステムにおけるサーバ装置の構成と、本実施の形態６によるフィルタリングの処理手順とを説明する。

【０１４２】

（１）サーバ装置の構成

まず最初に、本実施の形態６に係るサーバクライアントシステムにおけるサーバ装置の構成を説明する。図１１は、本実施の形態６に係るサーバクライアントシステムの構成を示すブロック図である。同図に示すように、本実施の形態６におけるサーバ装置１１０は、Ｗｅｂサーバ４０と、リクエストフィルタ１１１とを備え、さらに、このリクエストフィルタ１１１は、受信部３１と、見積部３２と、不正リクエストＤＢ３３と、判定部３４と、送信部３５と、レスポンス受信部１１２と、レスポンス見積部１１３と、不正レスポンスＤＢ１１４と、レスポンス判定部１１５と、レスポンス送信部１１６とを備える。

【０１４３】

このうち、受信部３１、見積部３２、不正リクエストＤＢ３３、判定部３４および送信部３５は、図１に示した同一符号を付している各部と同様の機能を有し、上記実施の形態１または２に示したフィルタリング処理と同様の処理、すなわち、パターンに基づくフィルタリング処理を実行するものである。

【０１４４】

ところで、Ｗｅｂサーバ４０が所有しないファイルを要求するＨＴＴＰリクエ

ストなど、不正アクセスのパターンとして記述することが困難なＨＴＴＰリクエストについては、不正リクエストＤＢ３３にはパターンとして格納されないので、不正リクエストとして破棄されることなく、Ｗｅｂサーバ４０に送信されることとなる。しかしながら、かかる不正リクエストに応じてＷｅｂサーバ４０からクライアント装置１０に送信されようとするレスポンスは、以下に説明する各部の処理によって、不正なレスポンスとして破棄される。

【０１４５】

レスポンス受信部１１２は、Ｗｅｂサーバ４０からのレスポンスをクライアント装置１０に送信する前に受信する処理部である。なお、レスポンス受信部１１２によりＷｅｂサーバ４０から受信したレスポンスは、レスポンス見積部１１３およびレスポンス送信部１１６に出力される。

【０１４６】

レスポンス見積部１１３は、不正レスポンスＤＢ１１４に格納された不正レスポンスのパターンおよび所定の見積ルール１１３ａに基づいてレスポンスの正当性を見積もり、その見積結果をレスポンス判定部１１５に出力する処理部である。

【０１４７】

ここで、上記の不正レスポンスＤＢ１１４は、ＨＴＴＰリクエストに応じてＷｅｂサーバ４０からクライアント装置１０に対してサービスとして送信されるレスポンスのうち、クライアント装置１０に対して送信されるべきでない不正レスポンスのパターンを格納したデータベースである。具体的には、ディレクトリ情報など、Ｗｅｂサーバ４０の外部に漏れてはいけない秘匿情報をパターンとして記憶する。

【０１４８】

これらの秘匿情報をパターンとして記憶することとしたのは、Ｗｅｂサーバ４０が所有しないファイルを要求するＨＴＴＰリクエストに対するレスポンスとして、これらの秘匿情報がクライアント装置１０に送信されるおそれがあるからである。

【０１４９】

そして、レスポンス見積部１１３は、このような秘匿情報を格納した不正レスポンスＤＢ１１４を参照することにより、所定の見積ルール１１３ａに基づいてレスポンスの正当性の見積もりをおこなう。具体的には、レスポンスが不正レスポンスＤＢ１１４に格納された秘匿情報パターンのいずれかに該当する場合には、該レスポンスは不正レスポンスである旨を見積もり、一方、レスポンスが不正レスポンスＤＢ１１４に格納された秘匿情報パターンのいずれにも該当しない場合には、該レスポンスは正当レスポンスである旨を見積もる。

【０１５０】

レスポンス判定部１１５は、レスポンス見積部１１３から受け取った見積結果および所定の判定ルール１１５ａに基づいてレスポンスをクライアント装置１０に送信するか否かを判定し、この判定結果をレスポンス送信部１１６に出力する処理部である。具体的には、レスポンス見積部１１３から不正レスポンスである旨の見積結果を受け取った場合には、レスポンスをクライアント装置１０に送信しないものと判定し（不可判定）、一方、レスポンス見積部１１３から正当レスポンスである旨の見積結果を受け取った場合には、レスポンスをクライアント装置１０に送信するものと判定する（可判定）。

【０１５１】

レスポンス送信部１１６は、レスポンス判定部１１５から受け取った判定結果に基づいて、レスポンス受信部１１２から受け取ったレスポンスの送信を制御する処理部である。具体的には、レスポンス判定部１１５から可判定を受け取った場合には、レスポンスをネットワーク１を介してクライアント装置１０に送信する。一方、レスポンス判定部１１５から不可判定を受け取った場合には、レスポンスのクライアント装置１０への送信を拒絶して、このレスポンスを不正レスポンスとして破棄する。

【０１５２】

なお、図７には図示していないが、本実施の形態６のリクエストフィルタ１１１は、図１に示した実施の形態１のリクエストフィルタ３０と同様、ログ管理部、外部通信部、外部情報取得部および更新部を備えるものである。すなわち、本実施の形態６のリクエストフィルタ１１１においては、実施の形態１のリクエス

トフィルタ３０と同様、ログ管理部は、所定の格納ルールに基づいて、レスポンス送信部１１６によりクライアント装置１０に送信されなかったレスポンスに係る情報や、このレスポンスの起因となったＨＴＴＰリクエストに係る情報を所定の格納媒体に格納して管理する。

【０１５３】

また、外部通信部は、所定の通報ルールに基づいて、レスポンス送信部１１６によりクライアント装置１０に送信されなかったレスポンスに係る情報や、このレスポンスの起因となったＨＴＴＰリクエストに係る情報を外部装置に通報する。さらに、外部情報取得部は、所定の取得ルールに基づいて、更新部による更新処理に用いられる情報を、外部装置やＷｅｂサーバ４０などのリクエストフィルタ１１１の外部から能動的または受動的に取得する。

【０１５４】

そして、更新部は、所定の更新ルールに基づいて、不正レスポンスＤＢ１１４、見積ルール１１３ａ、判定ルール１１５ａ、管理ルール、通報ルール、取得ルールまたは更新ルールに格納された情報を更新する。例えば、外部情報取得部から新たな不正レスポンスのパターンを受け付けた場合には、この不正レスポンスのパターンを不正レスポンスＤＢ１１４に格納し、また見積ルール１１３ａの変更指示情報を受け付けた場合には、この変更指示情報に応じて見積ルール１１３ａを変更する。

【０１５５】

（２）フィルタリング処理

次に、本実施の形態６によるフィルタリングの処理手順について説明する。図１２は、本実施の形態６によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置１１０におけるリクエストフィルタ１１１の受信部３１は、クライアント装置１０からのＨＴＴＰリクエストをＷｅｂサーバ４０が受信する前に受信する（ステップＳ１２０１）。

【０１５６】

続いて、リクエストフィルタ１１１は、このＨＴＴＰリクエストを見積部３２に受け渡し、上記実施の形態１または２によるフィルタリング処理と同様の処理

、すなわち、パターンに基づくフィルタリング処理を実行する（ステップＳ１２０２～Ｓ１２０５、ステップＳ１２１０およびＳ１２１１）。

【０１５７】

すなわち、見積部３２は、不正リクエストＤＢ３３に格納されたサーバに対する不正アクセスのパターンに基づいて、ＨＴＴＰリクエストの正当性を見積もり（ステップＳ１２０２）、判定部３４は、ＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡すか否か（すなわち、正当リクエストである旨が見積もられたか否か、または見積値ＤＩが所定の閾値以下であるか否か）を判定する（ステップＳ１２０３）。

【０１５８】

この判定により、ＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡さないものと判定された場合（すなわち、不正リクエストである旨が見積もられた場合、または見積値ＤＩが所定の閾値以上である場合）には（ステップＳ１２０３否定）、送信部３５は、ＨＴＴＰリクエストのＷｅｂサーバ４０への受け渡しを拒絶する（ステップＳ１２１０）。さらに、リクエストフィルタ１１１の各部は、不正リクエストの破棄、格納媒体への格納、外部装置への通報などの不正判定時の処理をおこなう（ステップＳ１２１１）。

【０１５９】

これとは反対に、正当リクエストである旨が見積もられた場合には（ステップＳ１２０３肯定）、送信部３５は、ＨＴＴＰリクエストをプロセス間通信によりＷｅｂサーバ４０に送信し（ステップＳ１２０４）、Ｗｅｂサーバ４０は、ＨＴＴＰリクエストに応じたレスポンスを作成するなど、正当判定時の処理をおこなう（ステップＳ１２０５）。

【０１６０】

続いて、リクエストフィルタ１１１のレスポンス受信部１１２は、Ｗｅｂサーバ４０からレスポンスを受信する（ステップＳ１２０６）。そして、レスポンス見積部１１３は、不正レスポンスＤＢ１１４に格納された秘匿情報パターンおよび所定の見積ルール１１３ａに基づいてレスポンスの正当性を見積もる（ステップＳ１２０７）。具体的には、レスポンスが不正レスポンスＤＢ１１４に格納さ

れた秘匿情報パターンのいずれかに該当する場合には、該レスポンスは不正レスポンスである旨を見積もり、一方、レスポンスが不正レスポンスＤＢ１１４に格納された秘匿情報パターンのいずれにも該当しない場合には、該レスポンスは正当レスポンスである旨を見積もる。

【０１６１】

その後、レスポンス判定部１１５は、レスポンス見積部１１３から受け取った見積結果および所定の判定ルール１１５ａに基づいて、レスポンスをクライアント装置１０に送信するか否かを判定する（ステップＳ１２０８）。具体的には、正当なレスポンスとして見積もられたか否かを判定する。

【０１６２】

この判定により、正当なレスポンスである旨が見積もられたものと判定された場合には（ステップＳ１２０８肯定）、レスポンス送信部１１６は、レスポンスをネットワーク１を介してクライアント装置１０に送信する（ステップＳ１２０９）。

【０１６３】

これとは反対に、不正なレスポンスである旨が見積もられたものと判定された場合には（ステップＳ１２０８否定）、レスポンス送信部１１６は、レスポンスのクライアント装置１０への送信を拒絶し（ステップＳ１２１２）、リクエストフィルタ１１１の各部は、不正レスポンスの破棄、格納媒体への格納、外部装置への通報など、不正判定時の処理をおこなう（ステップＳ１２１３）。

【０１６４】

上記した一連の処理によって、正当なアクセスに応じた正当なレスポンス、すなわち不正アクセスとして破棄されず、かつ、不正レスポンスとして破棄されなかったレスポンスのみが、クライアント装置１０に送信されることとなる。

【０１６５】

上述してきたように、本実施の形態６によれば、クライアント装置１０から送信されたＨＴＴＰリクエストに対して種々の見積もりをおこなって不正アクセスを破棄するとともに、ＨＴＴＰリクエストに応じてＷｅｂサーバ４０からクライアント装置１０に送信されるレスポンスに対しても、その正当性を見積もって不

正なレスポンスを破棄することとしたので、不正アクセスのパターンとして記述される不正アクセスのみならず、不正アクセスのパターンとして記述し難い不正アクセスに応じた不正なレスポンスをも破棄することができる。これによって、クライアント装置１０による不正アクセスからＷｅｂサーバ４０を一層確実に防御することができる。

【０１６６】

（３）本実施の形態６の変形例

さて、これまで本実施の形態６について説明したが、本発明は上述した実施の形態６以外にも、上記特許請求の範囲に記載した技術的思想の範囲内において種々の異なる実施の形態にて実施されてもよいものである。

【０１６７】

例えば、本実施の形態６では、Ｗｅｂサーバ４０からのレスポンスが不正レスポンスＤＢ１１４に格納された不正レスポンスのパターンに該当するか否かによって不正レスポンスであるか否かを判定する場合について説明したが、本発明はこれに限定されるものではなく、不正レスポンスＤＢ１１４に格納された不正レスポンスのパターンに該当する度合に応じて不正レスポンスであるか否かを判定する場合にも同様に適用することができる。

【０１６８】

すなわち、この場合には、上記実施の形態２と同様、レスポンス見積部１１３は、不正レスポンスＤＢ１１４に格納された不正レスポンスのパターンから一致するパターンの個数を算出することや、各パターンに危険度数を付与して一致するパターンの危険度数を算出することなどにより、レスポンスの危険度を示すＤＩ（Danger　Index）と呼ばれる見積値を算出し、レスポンス判定部１１５は、この算出された見積値と所定の閾値とを比較してレスポンスをクライアント装置１０に送信するか否かを判定することとなる。

【０１６９】

また、本実施の形態６では、クライアント装置１０から送信されたＨＴＴＰリクエストに対しては、パターンに基づくフィルタリング処理を実行する場合を説明したが、本発明はこれに限定されるものではなく、上記実施の形態３で説明し

た事前判定処理や、上記実施の形態４で説明した統計に基づくフィルタリング処理をともに実行する場合にも同様に適用することができる。

【０１７０】

（実施の形態７）

ところで、上記実施の形態１～６では、暗号処理されていないＨＴＴＰリクエストや暗号処理されていないレスポンスに対してフィルタリング処理を実行する場合を説明したが、本発明はこれに限定されるものではなく、暗号処理がなされたＨＴＴＰリクエストや暗号処理がなされたレスポンスに対してフィルタリング処理を実行する場合にも同様に適用することができる。

【０１７１】

すなわち、上記実施の形態１～６では、Ｗｅｂサーバ４０が、クライアント装置１０から暗号処理されていないＨＴＴＰリクエストを受信するとともに、暗号処理されていないレスポンスをクライアント装置１０に送信することを前提にしている。しかしながら、Ｗｅｂサーバ４０によっては、提供するサービスの秘匿性などを確保するために、クライアント装置１０から暗号処理がなされたＨＴＴＰリクエストを受信するとともに、暗号処理がなされてたレスポンスをクライアント装置１０に送信するようにしたものもある。

【０１７２】

このようなＷｅｂサーバ４０に対して、上記実施の形態１～６で説明したフィルタリング処理を単純に適用したのでは、暗号化がなされた不正アクセスや暗号化がなされた不正レスポンスを破棄することはできない。このため、不正アクセスからＷｅｂサーバ４０を防御することができず、さらに、Ｗｅｂサーバ４０からクライアント装置１０に不正レスポンスが送信されるおそれがある。

【０１７３】

そこで、本実施の形態７では、暗号処理がなされたＨＴＴＰリクエストを復号するとともに、暗号処理がなされたレスポンスを復号することによって、暗号化がなされた不正アクセスや暗号化がなされた不正レスポンスをも破棄することができるようにしている。以下、本実施の形態７に係るサーバクライアントシステムにおけるサーバ装置の構成を説明する。

【０１７４】

図１３は、本実施の形態７に係るサーバクライアントシステムの構成を示すブロック図である。なお、図１または図１１に示した各部と同様の機能を有する部位には同一符号を付すこととしてその詳細な説明を省略し、本実施の形態７の特徴部分である復号部１２２および復号部１２３について説明する。

【０１７５】

サーバ装置１２０におけるリクエストフィルタ１２１の復号部１２２は、所定の暗号処理がなされたＨＴＴＰリクエストを復号する復号手段である。具体的には、受信部３１から暗号処理がなされたＨＴＴＰリクエストを受け取った後、このＨＴＴＰリクエストを復号し、復号したＨＴＴＰリクエストを見積部３２に出力する。これによって、見積部３２は、上記実施の形態１または２で説明した見積処理を実行することとなる。

【０１７６】

なお、受信部３１は、暗号処理がなされたＨＴＴＰリクエストを送信部３５に出力するので、Ｗｅｂサーバ４０には、暗号処理がなされたＨＴＴＰリクエストが送信されることとなる。これによって、一つのリクエストフィルタ１２１により複数のＷｅｂサーバ４０を防御するために、リクエストフィルタ１２１と複数のＷｅｂサーバ４０とをインターネットなどの非専用回線で接続した場合でも、ＨＴＴＰリクエストの秘匿性を確保することができる。

【０１７７】

一方、復号部１２３は、所定の暗号処理がなされたレスポンスを復号する第２の復号手段である。具体的には、レスポンス受信部１１２から暗号処理がなされたレスポンスを受け取った後、このレスポンスを復号し、復号したレスポンスをレスポンス見積部１１３に出力する。これによって、レスポンス見積部１１３は、上記実施の形態６で説明した見積処理を実行することとなる。

【０１７８】

なお、レスポンス受信部１１２は、暗号処理がなされたレスポンスをレスポンス送信部１１６に出力するので、クライアント装置１０には、暗号処理がなされたレスポンスが送信されることとなる。これによって、クライアント装置１０に

送信されるレスポンスの秘匿性を確保することができる。

【０１７９】

上述してきたように、本実施の形態７によれば、暗号処理がなされたＨＴＴＰリクエストを復号するとともに、暗号処理がなされたレスポンスを復号することとしたので、クライアント装置１０から暗号処理がなされたＨＴＴＰリクエストを受信するとともに、暗号処理がなされてたレスポンスをクライアント装置１０に送信するようにしたＷｅｂサーバ４０に適用する場合においても、暗号化がなされた不正アクセスや暗号化がなされた不正レスポンスを破棄することができる。これによって、不正アクセスからＷｅｂサーバ４０を確実に防御することができ、さらに、Ｗｅｂサーバ４０からクライアント装置１０に不正レスポンスが送信されるおそれを確実に排除することができる。

【０１８０】

なお、本実施の形態７では、ＨＴＴＰリクエストおよびレスポンスを復号する場合を説明したが、本発明はこれに限定されるものではなく、ＨＴＴＰリクエストのみを復号する場合や、レスポンスのみを復号する場合など、Ｗｅｂサーバ４０の処理態様（暗号処理がなされたＨＴＴＰリクエストを受信するか否か、暗号処理がなされたレスポンスを送信するか否かなど）に応じて、ＨＴＴＰリクエストまたはレスポンスの一方を復号する場合に同様に適用することができる。

【０１８１】

また、本実施の形態７では、リクエストフィルタ１２１によりＨＴＴＰリクエストを復号した後に、Ｗｅｂサーバ４０には、暗号処理がなされたＨＴＴＰリクエストを送信する場合を説明したが、本発明はこれに限定されるものではなく、Ｗｅｂサーバ４０に対して、復号されたＨＴＴＰリクエストを送信する場合にも同様に適用することができる。なお、この場合には、Ｗｅｂサーバ４０の復号手段を省略することができる。

【０１８２】

また、本実施の形態７では、クライアント装置１０から送信されたＨＴＴＰリクエストに対しては、パターンに基づくフィルタリング処理を実行する場合を説明したが、本発明はこれに限定されるものではなく、上記実施の形態３で説明し

た事前判定処理や、上記実施の形態４で説明した統計に基づくフィルタリング処理をともに実行する場合にも同様に適用することができる。なお、この場合にも、事前判定処理や統計に基づくフィルタリング処理に先だって、本実施の形態７で説明した復号処理が実行される。

【０１８３】

（実施の形態８）

ところで、上記実施の形態１～７では、不正なＨＴＴＰリクエストや不正なレスポンスを破棄する場合を説明したが、本発明はこれに限定されるものではなく、クライアント装置１０に対して、不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを送信することもできる。

【０１８４】

すなわち、不正なＨＴＴＰリクエストや不正なレスポンスを破棄するだけでは、不正アクセスを試行した攻撃者（クラッカー）は、不正アクセスが失敗したことに気づいて、新たな別の不正アクセスを試行するおそれがある。このため、望ましくは、不正アクセスが失敗したことを攻撃者に気づかせることなく時間を稼ぐことによって、新たな別の不正アクセスを未然に防止したり、攻撃者の攻撃手口を解析することが必要とされる。

【０１８５】

ところで、従来より、不正アクセスからサーバを保護する技術として、おとりシステム（おとりサーバ、ハニーポット）と呼ばれる技術が一般的に知られている。このおとりシステムは、セキュリティホールを有するといった脆弱なサーバを装って、攻撃者による不正アクセスの試行を全てロギングするものである。

【０１８６】

すなわち、攻撃者は一般的に、ネットワーク上のセキュリティレベルの低いサーバを攻撃対象とする行動志向を有するので、おとりシステムは、脆弱なサーバを装って、攻撃者がおとりシステムにアクセスしたならば、真のサーバ（不正アクセスから保護したいサーバ）であるかのようにログインバナーの返信などをする。そして、攻撃者が辞書を用いたパスワードクラッキングなどによってログインを試行してきた場合には、これらの行動を全てログとして安全に記録する。

【０１８７】

このようにして、おとりシステムは、真のサーバが攻撃されるまでの時間を稼ぎ、新たな別の不正アクセスを未然に防止したり、攻撃者の攻撃手口（攻撃に用いる辞書など）を解析する。そして、この攻撃手口の解析結果や時間稼ぎによって、真のサーバに対する防御策を講じることが可能になる。

【０１８８】

しかしながら、おとりシステムは、不正アクセスから保護したい真のサーバのおとりにはなれないという問題点がある。すなわち、あるサーバを保護しようとする場合、一般的に、おとりシステムは、そのサーバのミラーサーバ若しくはテストサーバを装って（それらを連想させる名前を付与されて）運用される。これは、真のサーバに対して正規にアクセスしようとする正規ユーザのために、真のサーバについては、真のサーバとわかる名前を付与して運用しなければならないからである。

【０１８９】

したがって、真のサーバを保護するために、おとりシステムを導入しても、攻撃者がおとりシステムに目もくれず、真のサーバを攻撃してきたような場合には、おとりシステムの機能は没却され、真のサーバを保護するという目的を達成することができなくなってしまう。

【０１９０】

そこで、本実施の形態８では、おとりシステムではなく、Ｗｅｂサーバ４０に対する不正アクセスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを格納した偽レスポンスデータベースを導入することによって、不正アクセスを試行したクライアント装置１０に対して、不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを送信することができるようにしている。以下、本実施の形態８に係るサーバクライアントシステムにおけるサーバ装置の構成と、本実施の形態８によるフィルタリングの処理手順とを説明する。

【０１９１】

（１）サーバ装置の構成

まず最初に、本実施の形態８に係るサーバクライアントシステムにおけるサーバ装置の構成を説明する。図１４は、本実施の形態８に係るサーバクライアントシステムの構成を示すブロック図である。同図に示すように、本実施の形態８におけるサーバ装置１３０は、Ｗｅｂサーバ４０と、リクエストフィルタ１３１とを備え、さらに、このリクエストフィルタ１３１は、受信部３１と、見積部３２と、不正リクエストＤＢ３３と、判定部３４と、送信部３５と、偽レスポンス作成部１３２と、偽レスポンスＤＢ１３３と、レスポンス送信部１３４とを備える。

【０１９２】

このうち、受信部３１、見積部３２、不正リクエストＤＢ３３、判定部３４および送信部３５は、図１に示した同一符号を付している各部と同様の機能を有し、上記実施の形態１または２に示したフィルタリング処理と同様の処理、すなわち、パターンに基づくフィルタリング処理を実行するものである。このフィルタリング処理によって、不正なＨＴＴＰリクエストは、Ｗｅｂサーバ４０に送信されることなく、偽レスポンス作成部１３２に出力される。

【０１９３】

偽レスポンス作成部１３２は、偽レスポンスＤＢ１３３および所定の作成ルールに基づいて、不正アクセスとしてＷｅｂサーバ４０に受け渡されなかったＨＴＴＰリクエストのパターンに対応した偽のレスポンスを作成する処理部である。

【０１９４】

ここで、上記の偽レスポンスＤＢ１３３は、Ｗｅｂサーバ４０に対する不正アクセスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを格納したデータベースである。具体的には、不正リクエストＤＢ３３に格納された不正アクセスのパターンに対応付けて偽のレスポンスを記憶する。例えば、Ｗｅｂサーバ４０上のパスワードファイルをリクエストする不正アクセスのパターンに対応付けられた、架空の情報からなる偽のパスワードファイルや、Ｗｅｂサーバ４０に不正にログインしようとする不正アクセスのパターンに対応付けられた、偽のログインバナーなどを記憶する。

【０１９５】

そして、偽レスポンス作成部１３２は、このような情報を格納した偽レスポンスＤＢ１３３を参照することにより、不正アクセスとしてＷｅｂサーバ４０に受け渡されなかったＨＴＴＰリクエストのパターンに対応した偽のレスポンスを作成する。

【０１９６】

具体的には、Ｗｅｂサーバ４０上のパスワードファイルをリクエストするＨＴＴＰリクエストが、不正アクセスとして偽レスポンス作成部１３２に入力された場合には、偽レスポンスＤＢ１３３に格納された偽のパスワードファイルを用いて偽のレスポンスを作成する。また、Ｗｅｂサーバ４０に不正にログインしようとするＨＴＴＰリクエストが、不正アクセスとして偽レスポンス作成部１３２に入力された場合には、偽レスポンスＤＢ１３３に格納された偽のログインバナーを用いて偽のレスポンスを作成する。

【０１９７】

レスポンス送信部１３４は、Ｗｅｂサーバ４０により正当に作成された正当レスポンスや、偽レスポンス作成部１３２により作成された偽のレスポンスをクライアント装置１０に送信する処理部である。なお、図１４には図示していないが、本実施の形態８のリクエストフィルタ１３１は、図１に示した実施の形態１のリクエストフィルタ３０と同様、ログ管理部、外部通信部、外部情報取得部および更新部を備えるものである。

【０１９８】

（２）フィルタリング処理

次に、本実施の形態８によるフィルタリングの処理手順について説明する。図１５は、本実施の形態８によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置１３０におけるリクエストフィルタ１３１の受信部３１は、クライアント装置１０からのＨＴＴＰリクエストをＷｅｂサーバ４０が受信する前に受信する（ステップＳ１５０１）。

【０１９９】

続いて、リクエストフィルタ１３１は、このＨＴＴＰリクエストを見積部３２に受け渡し、上記実施の形態１または２によるフィルタリング処理と同様の処理

、すなわち、パターンに基づくフィルタリング処理を実行する（ステップＳ１５０２～Ｓ１５０５、ステップＳ１５０７およびＳ１５０８）。

【０２００】

すなわち、見積部３２は、不正リクエストＤＢ３３に格納されたサーバに対する不正アクセスのパターンに基づいて、ＨＴＴＰリクエストの正当性を見積もり（ステップＳ１５０２）、判定部３４は、ＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡すか否か（すなわち、正当リクエストである旨が見積もられたか否か、または見積値ＤＩが所定の閾値以下であるか否か）を判定する（ステップＳ１５０３）。

【０２０１】

この判定により、正当リクエストである旨が見積もられた場合には（ステップＳ１５０３肯定）、送信部３５は、ＨＴＴＰリクエストをプロセス間通信によりＷｅｂサーバ４０に送信し（ステップＳ１５０４）、Ｗｅｂサーバ４０は、ＨＴＴＰリクエストに応じたレスポンスを作成するなど、正当判定時の処理をおこなう（ステップＳ１５０５）。続いて、レスポンス送信部１３４は、Ｗｅｂサーバ４０により作成されたレスポンスをクライアント装置１０に送信する（ステップＳ１５０６）

【０２０２】

これとは反対に、ＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡さないものと判定された場合（すなわち、不正リクエストである旨が見積もられた場合、または見積値ＤＩが所定の閾値以上である場合）には（ステップＳ１５０３否定）、送信部３５は、ＨＴＴＰリクエストのＷｅｂサーバ４０への受け渡しを拒絶する（ステップＳ１５０７）。さらに、リクエストフィルタ１３１の各部は、不正リクエストの破棄、格納媒体への格納、外部装置への通報などの不正判定時の処理をおこなう（ステップＳ１５０８）。

【０２０３】

続いて、偽レスポンス作成部１３２は、偽レスポンスＤＢ１３３および所定の作成ルール１３２ａに基づいて、不正アクセスとしてＷｅｂサーバ４０に受け渡されなかったＨＴＴＰリクエストのパターンに対応した偽のレスポンスを作成す

る（ステップＳ１５０９）。具体的には、偽レスポンスＤＢ１３３に格納された偽のパスワードファイルを用いた偽のレスポンスや、偽レスポンスＤＢ１３３に格納された偽のログインバナーを用いた偽のレスポンスなどを作成する。その後、レスポンス送信部１３４は、偽レスポンス作成部１３２により作成された偽のレスポンスをクライアント装置１０に送信する（ステップＳ１５１０）。

【０２０４】

上記した一連の処理によって、不正アクセスのパターンに該当するＨＴＴＰリクエストをＷｅｂサーバ４０に送信してきたクライアント装置１０に対して、不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを送信されることとなる。

【０２０５】

上述してきたように、本実施の形態８によれば、Ｗｅｂサーバ４０に対する不正アクセスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを格納した偽レスポンスＤＢ１３３を導入することとしたので、不正アクセスを試行したクライアント装置１０に対して、不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを送信することができる。これによって、不正アクセスが失敗したことを攻撃者に気づかせることなく時間を稼ぐことができ、さらに、新たな別の不正アクセスを未然に防止したり、攻撃者の攻撃手口を解析することもできるので、クライアント装置１０による不正アクセスからＷｅｂサーバ４０を一層確実に防御することが可能になる。

【０２０６】

なお、本実施の形態８では、クライアント装置１０から送信されたＨＴＴＰリクエストに対しては、パターンに基づくフィルタリング処理を実行する場合を説明したが、本発明はこれに限定されるものではなく、上記実施の形態３で説明した事前判定処理や、上記実施の形態４で説明した統計に基づくフィルタリング処理、さらには、上記実施の形態６で説明したレスポンスのフィルタリング処理をともに実行する場合にも同様に適用することができる。

【０２０７】

すなわち、例えば、上記実施の形態６で説明したレスポンスのフィルタリング

処理をともに実行する場合には、偽レスポンスＤＢ１３３に、不正なレスポンスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンス（例えば、偽のディレクトリ情報など）を格納することとなる。

【０２０８】

ただし、上記実施の形態４で説明した統計に基づくフィルタリング処理をともに実施する場合には、かかるフィルタリング処理により破棄されたＨＴＴＰレスポンスについては、偽レスポンスを作成しないようにすることも有効である。このようなサーバダウンを狙ったＨＴＴＰレスポンスに対して偽レスポンスを作成したのでは、偽レスポンス作成処理の負担が却って増大してしまうからである。

【０２０９】

（実施の形態９）

ところで、上記実施の形態８では、Ｗｅｂサーバ４０に対する不正アクセスのパターンに対応する偽のレスポンスを格納した偽レスポンスＤＢ１３３を参照して、偽レスポンスを作成する場合を説明したが、本発明はこれに限定されるものではなく、不正アクセスとしてＷｅｂサーバ４０に受け渡されなかったＨＴＴＰリクエストを受け入れて、Ｗｅｂサーバ４０のおとりとして機能する偽Ｗｅｂサーバによって、偽のレスポンスを作成することもできる。

【０２１０】

すなわち、Ｗｅｂサーバ４０に対する不正アクセスには、パターンとして把握できないものもあり、このような不正アクセスについては、上記実施の形態８で説明した偽レスポンスＤＢ１３３を参照して偽レスポンスを作成することできない。このため、不正アクセスが失敗したことを攻撃者に気づかせることなく時間を稼ぐこともできず、さらに、新たな別の不正アクセスを未然に防止したり、攻撃者の攻撃手口を解析することもできなくなってしまう。

【０２１１】

そこで、本実施の形態９では、偽レスポンスＤＢ１３３ではなく、不正なアクセスとしてＷｅｂサーバ４０に受け渡されなかったＨＴＴＰリクエストを受け入れて、Ｗｅｂサーバ４０のおとりとして該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを作成する偽Ｗｅｂサーバを導入することによって

、パターンとして把握できない不正アクセスに対しても、偽のレスポンスを送信することができるようにしている。以下、本実施の形態９に係るサーバクライアントシステムにおけるサーバ装置の構成と、本実施の形態９によるフィルタリングの処理手順とを説明する。

【０２１２】

図１６は、本実施の形態９に係るサーバクライアントシステムの構成を示すブロック図である。なお、図１４に示した各部と同様の機能を有する部位には同一符号を付すこととしてその詳細な説明を省略し、本実施の形態９の特徴部分である偽Ｗｅｂサーバ１４２について説明する。

【０２１３】

サーバ装置１４０におけるリクエストフィルタ１４１の偽Ｗｅｂサーバ１４２は、不正なアクセスとしてＷｅｂサーバ４０に受け渡されなかったＨＴＴＰリクエストを受け入れて、Ｗｅｂサーバ４０のおとりとして該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを作成する処理部である。具体的には、Ｗｅｂサーバ４０と同様、ＨＴＴＰリクエストに応じてＨＴＭＬ（HyperText Markup Language）などのマークアップ言語により記述された各種の情報を送信するなどのサービスをクライアント装置１０に提供するものであるが、Ｗｅｂサーバ４０のおとりとして、偽のサービスを提供（偽のレスポンスを作成）するように偽のデータを所有する。

【０２１４】

例えば、Ｗｅｂサーバ４０上のパスワードファイルをリクエストする不正なＨＴＴＰリクエストを受け入れて、偽のパスワードファイルを作成したり、コマンド文字列を含んだリクエストによりＷｅｂサーバ４０上で任意のシステムコマンドを実行するなどの不正なＨＴＴＰリクエストを受け入れて、そのシステムコマンドを実行したり、Ｗｅｂサーバ４０上に存在しないファイルをリクエストしてＷｅｂサーバ４０の機能を停止させる不正なＨＴＴＰリクエストを受け入れて、その機能を停止させる処理などをおこなう。

【０２１５】

すなわち、偽Ｗｅｂサーバ１４２は、不正なＨＴＴＰリクエストを受け入れて

、そのＨＴＴＰリクエストに応じた処理を実行するものであるが、Ｗｅｂサーバ４０のおとりとして偽のデータを所有するものであるため、偽Ｗｅｂサーバ１４２からのレスポンスは、不正なＨＴＴＰリクエストを受け入れたＷｅｂサーバ４０からのレスポンスと同様のものであるが、偽のレスポンスとなる。

【０２１６】

次に、本実施の形態９によるフィルタリングの処理手順について説明する。図１７は、本実施の形態９によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置１４０におけるリクエストフィルタ１４１は、クライアント装置１０からのＨＴＴＰリクエストをＷｅｂサーバ４０が受信する前に受信して（ステップＳ１７０１）、上記実施の形態８によるフィルタリング処理と同様の処理（図１５に示したステップＳ１５０１～Ｓ１５０８）を実行する（ステップＳ１７０１～ステップＳ１７０８）。

【０２１７】

このステップＳ１７０８に示すように、リクエストフィルタ１４１の各部は、不正リクエストの破棄、格納媒体への格納、外部装置への通報などの不正判定時の処理をおこなうと（ステップＳ１７０８）、続いて、送信部３５は、不正アクセスとしてＷｅｂサーバ４０に受け渡されなかったＨＴＴＰリクエストを、偽Ｗｅｂサーバ１４２に送信する（ステップＳ１７０９）。

【０２１８】

そして、偽Ｗｅｂサーバ１４２は、Ｗｅｂサーバ４０のおとりとして該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを作成する（ステップＳ１７１０）。具体的には、Ｗｅｂサーバ４０上のパスワードファイルをリクエストする不正なＨＴＴＰリクエストを受け入れて、偽のパスワードファイルを作成したり、コマンド文字列を含んだリクエストによりＷｅｂサーバ４０上で任意のシステムコマンドを実行するなどの不正なＨＴＴＰリクエストを受け入れて、そのシステムコマンドを実行したりなどする。その後、レスポンス送信部１３４は、偽Ｗｅｂサーバ１４２により作成された偽のレスポンスをクライアント装置１０に送信する（ステップＳ１７１１）。

【０２１９】

上記した一連の処理によって、不正アクセスのパターンとして把握できないＨＴＴＰリクエストをＷｅｂサーバ４０に送信してきたクライアント装置１０に対しても、不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを送信されることとなる。

【０２２０】

上述してきたように、本実施の形態９によれば、不正なアクセスとしてＷｅｂサーバ４０に受け渡されなかったＨＴＴＰリクエストを受け入れて、Ｗｅｂサーバ４０のおとりとして該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを作成する偽Ｗｅｂサーバ１４２を導入することとしたので、パターンとして把握できない不正アクセスに対しても、偽のレスポンスを送信することができる。特に、上記実施の形態８で説明したおとりシステムと異なり、偽Ｗｅｂサーバ１４２は、不正アクセスから保護したいＷｅｂサーバ４０のミラーサーバ若しくはテストサーバを装って運用される必要がないので、実質的にＷｅｂサーバ４０のおとりになれる点でも有効であると考えられる。

【０２２１】

なお、本実施の形態９においても、クライアント装置１０から送信されたＨＴＴＰリクエストに対しては、パターンに基づくフィルタリング処理を実行する場合を説明したが、本発明はこれに限定されるものではなく、上記実施の形態８と同様、上記実施の形態３で説明した事前判定処理や、上記実施の形態４で説明した統計に基づくフィルタリング処理、さらには、上記実施の形態６で説明したレスポンスのフィルタリング処理をともに実行する場合にも同様に適用することができる。

【０２２２】

（実施の形態１０）

ところで、上記実施の形態８および９では、Ｗｅｂサーバ４０に受け渡されなかった不正なＨＴＴＰリクエストのパターンに対応した偽のレスポンスを作成する場合と、不正なＨＴＴＰリクエストを受け入れて、Ｗｅｂサーバ４０のおとりとして偽のレスポンスを作成する場合とを説明したが、本発明はこれに限定されるものではなく、これらの両者をともに実行する場合にも同様に適用することが

できる。

【０２２３】

すなわち、上記実施の形態９では、Ｗｅｂサーバ４０に受け渡されなかった不正なＨＴＴＰリクエストの全てを偽Ｗｅｂサーバ１４２に受け渡すことによって、偽のレスポンスを作成することとしたが、不正アクセスのパターンとして把握できる不正なＨＴＴＰリクエストについても偽Ｗｅｂサーバ１４２に受け渡したのでは、偽Ｗｅｂサーバ１４２に過度な負担が強いられることとなる。

【０２２４】

そこで、本実施の形態１０では、不正アクセスのパターンとして把握できる不正なＨＴＴＰリクエストについては、不正レスポンスＤＢ１３３を参照して偽レスポンスを作成する一方、不正アクセスのパターンとして把握できない不正なＨＴＴＰリクエストについては、偽Ｗｅｂサーバ１４２により偽レスポンスを作成することとし、偽レスポンスを効率的かつ迅速に作成することができるようにしている。以下、本実施の形態１０に係るサーバクライアントシステムにおけるサーバ装置の構成と、本実施の形態１０によるフィルタリングの処理手順とを説明する。

【０２２５】

図１８は、本実施の形態１０に係るサーバクライアントシステムの構成を示すブロック図である。なお、図１４または１６に示した各部と同様の機能を有する部位には同一符号を付すこととしてその詳細な説明を省略し、本実施の形態１０の特徴部分である偽レスポンス作成部１５２について説明する。

【０２２６】

サーバ装置１５０におけるリクエストフィルタ１５１の偽レスポンス作成部１５２は、偽レスポンスＤＢ１３３および所定の作成ルール１５２ａに基づいて、不正アクセスとしてＷｅｂサーバ４０に受け渡されなかったＨＴＴＰリクエストのパターンに対応した偽のレスポンスを作成するとともに、偽のレスポンスが作成できなかったＨＴＴＰリクエストを偽Ｗｅｂサーバ１４２に受け渡す処理部である。

【０２２７】

具体的には、偽レスポンス作成部１５２は、不正アクセスとしてＷｅｂサーバ４０に受け渡されなかったＨＴＴＰリクエストを送信部３５から受け付け、このＨＴＴＰリクエストのパターンが偽レスポンスＤＢ１３３に格納されている不正リクエストのパターンに該当するか否かを判定する。そして、このパターンに該当する場合には、上記実施の形態８と同様、偽レスポンスＤＢ１３３に基づいて偽レスポンスを作成する。一方、このパターンに該当しない場合には、ＨＴＴＰリクエストを偽Ｗｅｂサーバ１４２に受け渡し、偽Ｗｅｂサーバ１４２に、上記実施の形態９の同様、Ｗｅｂサーバ４０のおとりとして偽レスポンスを作成させる。

【０２２８】

次に、本実施の形態１０によるフィルタリングの処理手順について説明する。図１９は、本実施の形態１０によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置１５０におけるリクエストフィルタ１５１は、クライアント装置１０からのＨＴＴＰリクエストをＷｅｂサーバ４０が受信する前に受信して（ステップＳ１９０１）、上記実施の形態８によるフィルタリング処理と同様の処理（図１５に示したステップＳ１５０１～Ｓ１５０８）を実行する（ステップＳ１９０１～ステップＳ１９０８）。

【０２２９】

このステップＳ１９０８に示すように、リクエストフィルタ１５１の各部は、不正リクエストの破棄、格納媒体への格納、外部装置への通報などの不正判定時の処理をおこなうと（ステップＳ１９０８）、続いて、偽レスポンス作成部１５２は、破棄されたＨＴＴＰリクエストのパターンが偽レスポンスＤＢ１３３に格納されている不正リクエストのパターンに該当するか否かを判定する（ステップＳ１９０９）。

【０２３０】

この判定により、不正リクエストのパターンに該当する場合には（ステップＳ１９０９肯定）、偽レスポンス作成部１５２は、偽レスポンスＤＢ１３３および所定の作成ルール１５２ａに基づいて、不正アクセスとしてＷｅｂサーバ４０に受け渡されなかったＨＴＴＰリクエストのパターンに対応した偽のレスポンスを

作成する（ステップＳ１９１０）。そして、レスポンス送信部１３４は、偽レスポンス作成部１５２により作成された偽のレスポンスをクライアント装置１０に送信する（ステップＳ１９１１）。

【０２３１】

これとは反対に、不正リクエストのパターンに該当しない場合には（ステップＳ１９０９否定）偽レスポンス作成部１５２は、パターンに該当しなかったＨＴＴＰリクエストを偽Ｗｅｂサーバ１４２に送信する（ステップＳ１９１２）。そして、偽Ｗｅｂサーバ１４２は、Ｗｅｂサーバ４０のおとりとして該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを作成する（ステップＳ１９１３）。その後、レスポンス送信部１３４は、偽Ｗｅｂサーバ１４２により作成された偽のレスポンスをクライアント装置１０に送信する（ステップＳ１９１１）。

【０２３２】

上記した一連の処理によって、不正アクセスのパターンとして把握できる不正なＨＴＴＰリクエストについては、不正レスポンスＤＢ１３３を参照して偽レスポンスが作成される一方、不正アクセスのパターンとして把握できない不正なＨＴＴＰリクエストについては、偽Ｗｅｂサーバ１４２により偽レスポンスが作成されることとなる。

【０２３３】

上述してきたように、本実施の形態１０によれば、不正アクセスのパターンとして把握できる不正なＨＴＴＰリクエストについては、不正レスポンスＤＢ１３３を参照して偽レスポンスを作成する一方、不正アクセスのパターンとして把握できない不正なＨＴＴＰリクエストについては、偽Ｗｅｂサーバ１４２により偽レスポンスを作成することとしたので、偽Ｗｅｂサーバ１４２に過度な負担を強いることなく、偽レスポンスを効率的かつ迅速に作成することができる。

【０２３４】

なお、本実施の形態１０においても、クライアント装置１０から送信されたＨＴＴＰリクエストに対しては、パターンに基づくフィルタリング処理を実行する場合を説明したが、本発明はこれに限定されるものではなく、上記実施の形態８

および９と同様、上記実施の形態３で説明した事前判定処理や、上記実施の形態４で説明した統計に基づくフィルタリング処理、さらには、上記実施の形態６で説明したレスポンスのフィルタリング処理をともに実行する場合にも同様に適用することができる。

【０２３５】

（他の実施の形態）

さて、これまで本発明の実施の形態について説明したが、本発明は上述した実施の形態以外にも、上記特許請求の範囲に記載した技術的思想の範囲内において種々の異なる実施の形態にて実施されてもよいものである。

【０２３６】

例えば、本実施の形態４～１０では、クライアント装置１０からのＨＴＴＰリクエストをフィルタリングする場合について説明したが、本発明はこれに限定されるものではなく、ＦＴＰ（File Transfer Protocol）、ｔｅｌｎｅｔ、コンソールなど、クライアント装置１０からＷｅｂサーバ４０に入力されるあらゆる情報をフィルタリングする場合に同様に適用することができる。

【０２３７】

また、本実施の形態４～１０では、フィルタリング装置としてのリクエストフィルタをサーバ装置に設けた場合について説明したが、本発明はこれに限定されるものではなく、例えば、それぞれのクライアント装置側にリクエストフィルタを設けたり、一つのリクエストフィルタにより複数のＷｅｂサーバを防御するなど、クライアント装置とＷｅｂサーバとの間にリクエストフィルタが介在するあらゆるシステム構成において同様に適用することができる。

【０２３８】

なお、本実施の形態４～１０で説明したフィルタリング方法は、あらかじめ用意されたプログラムをパーソナル・コンピュータやワークステーションなどのコンピュータで実行することによって実現することができる。このプログラムは、インターネットなどのネットワークを介して配布することができる。また、このプログラムは、ハードディスク、フレキシブルディスク（ＦＤ）、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤなどのコンピュータで読み取り可能な記録媒体に記録され、コン

ピュータによって記録媒体から読み出されることによって実行することもできる。

【０２３９】

（付記１）クライアントと該クライアントからのアクセス要求に応じてサービスを提供するサーバとの間に介在し、前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに受け渡すフィルタリング装置において、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースと、

前記不正パターンデータベースに格納された不正アクセスのパターンおよび所定の第１の見積ルールに基づいて前記アクセス要求の正当性を見積もる第１の見積手段と、

前記第１の見積手段による見積結果および所定の第１の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する第１の判定手段と、

を備えたことを特徴とするフィルタリング装置。

【０２４０】

（付記２）前記第１の見積手段は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第１の判定手段は、前記第１の見積手段により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記第１の見積手段により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記１に記載のフィルタリング装置。

【０２４１】

（付記３）前記第１の見積手段は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、前記第１の判定手段は、前記第１の見積手段により算出された見積値と所定の閾値とを比較して前記アクセス要求を前記サーバに受け渡すか否かを

判定することを特徴とする付記１に記載のフィルタリング装置。

【０２４２】

（付記４）前記サーバに対する正当アクセスのパターンを格納した正当パターンデータベースと、前記第１の見積手段による正当性の見積もりの前に、前記アクセス要求が前記正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定する事前判定手段と、をさらに備え、前記第１の見積手段は、前記事前判定手段により正当アクセスのパターンに該当しないものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする付記１、２または３に記載のフィルタリング装置。

【０２４３】

（付記５）所定の第１の外部送信ルールに基づいて、前記第１の判定手段により前記サーバに受け渡さないものと判定されたアクセス要求を所定の外部装置に送信する第１の外部送信手段をさらに備えたことを特徴とする付記１～４のいずれか一つに記載のフィルタリング装置。

【０２４４】

（付記６）所定の第１の格納ルールに基づいて、前記第１の判定手段により前記サーバに受け渡さないものと判定されたアクセス要求を所定の格納媒体に格納する第１の格納手段をさらに備えたことを特徴とする付記１～５のいずれか一つに記載のフィルタリング装置。

【０２４５】

（付記７）所定の第１の更新ルールに基づいて、前記不正パターンデータベース、正当パターンデータベース、第１の見積ルール、第１の判定ルール、第１の外部送信ルール、第１の格納ルールまたは第１の更新ルールを更新する第１の更新手段をさらに備えたことを特徴とする付記１～６のいずれか一つに記載のフィルタリング装置。

【０２４６】

（付記８）前記サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求に関する情報を格納した統計的不正データベースと、前記統計的不正データベースに格納された情報および所定の第２の見積ルールに基づい

て前記アクセス要求の正当性を見積もる第２の見積手段と、前記見積手段による見積結果および所定の第２の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する第２の判定手段と、前記第１および第２の判定手段により前記サーバに受け渡すものと判定されたアクセス要求のみを正当なアクセス要求として前記サーバに受け渡すアクセス要求受渡手段と、をさらに備えたことを特徴とする付記１～７のいずれか一つに記載のフィルタリング装置。

【０２４７】

（付記９）前記統計的不正データベースは、前記サーバに対してアクセス要求を送信したクライアントのうち、所定時間内のアクセス要求数が所定数を超えたクライアントの送信元情報を格納するものであって、

前記第２の見積手段は、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第２の判定手段は、前記第２の見積手段により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記第２の見積手段により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記８に記載のフィルタリング装置。

【０２４８】

（付記１０）前記統計的不正データベースは、前記サーバに対して送信されたアクセス要求の要求内容のうち、所定時間内のアクセス要求数が所定数を超えた要求内容を格納するものであって、

前記第２の見積手段は、前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第２の判定手段は、前記第２の見積手段により不正アクセスである旨が見積もられたアクセス要求を前記サー

バに受け渡さないものと判定するとともに、前記第２の見積手段により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記８に記載のフィルタリング装置。

【０２４９】

（付記１１）前記統計的不正データベースは、前記サーバに対してアクセス要求を送信したクライアントのうち、所定時間内のアクセス要求数が所定数を超えたクライアントの送信元情報を格納するとともに、前記サーバに対して送信されたアクセス要求の要求内容のうち、所定時間内のアクセス要求数が所定数を超えた要求内容を格納するものであって、

前記第２の見積手段は、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれかに該当する場合または前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれにも該当しない場合および前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれかにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第２の判定手段は、前記第２の見積手段により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記第２の見積手段により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記８に記載のフィルタリング装置。

【０２５０】

（付記１２）前記統計的不正データベースは、前記サーバに対してアクセス要求を送信したクライアントのうち、所定時間内のアクセス要求数が所定数を超えたクライアントの送信元情報を格納するとともに、前記サーバに対して送信されたアクセス要求の要求内容のうち、所定時間内のアクセス要求数が所定数を超えた要求内容を格納するものであって、

前記第２の見積手段は、前記アクセス要求の送信元情報および要求内容が前記統計的不正データベースに格納された送信元情報および要求内容に該当する度合

に応じて所定の見積値を算出し、前記第２の判定手段は、前記第２の見積手段により算出された見積値と所定の閾値とを比較して前記アクセス要求を前記サーバに受け渡すか否かを判定することを特徴とする付記８に記載のフィルタリング装置。

【０２５１】

（付記１３）前記第２の見積手段は、前記第１の判定手段により前記サーバに受け渡すものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする付記８～１２のいずれか一つに記載のフィルタリング装置。

【０２５２】

（付記１４）前記第１の見積手段は、前記第２の判定手段により前記サーバに受け渡すものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする付記８～１２のいずれか一つに記載のフィルタリング装置。

【０２５３】

（付記１５）前記事前判定手段は、前記第２の判定手段により前記サーバに受け渡すものと判定されたアクセス要求のみについて前記正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定することを特徴とする付記８～１２のいずれか一つに記載のフィルタリング装置。

【０２５４】

（付記１６）所定の第２の外部送信ルールに基づいて、前記アクセス要求受渡手段により前記サーバに受け渡されなかったアクセス要求を所定の外部装置に送信する第２の外部送信手段をさらに備えたことを特徴とする付記８～１５のいずれか一つに記載のフィルタリング装置。

【０２５５】

（付記１７）所定の第２の格納ルールに基づいて、前記アクセス要求受渡手段により前記サーバに受け渡されなかったアクセス要求を所定の格納媒体に格納する第２の格納手段をさらに備えたことを特徴とする付記８～１６のいずれか一つに記載のフィルタリング装置。

【０２５６】

（付記１８）所定の第２の更新ルールおよび／または前記サーバに対するアクセ

ス要求の統計に基づいて、前記統計的不正データベース、第２の見積ルール、第２の判定ルール、第２の外部送信ルール、第２の格納ルールおよび／または第２の更新ルールを更新する第２の更新手段をさらに備えたことを特徴とする付記８～１７のいずれか一つに記載のフィルタリング装置。

【０２５７】

（付記１９）前記第２の更新手段は、所定時間内に前記サーバに対してアクセス要求を送信した各クライアントごとのアクセス要求数および／または所定時間内に前記サーバに対して送信されたアクセス要求の各要求内容ごとのアクセス要求数に応じて、前記統計的不正データベースに格納される送信元情報および／または要求内容を追加および／または削除することを特徴とする付記１８に記載のフィルタリング装置。

【０２５８】

（付記２０）前記アクセス要求に応じて前記サーバから前記クライアントに対して前記サービスとして送信されるレスポンスのうち、前記クライアントに対して送信されるべきでない不正レスポンスのパターンを格納した不正レスポンスデータベースと、前記不正レスポンスデータベースに格納された不正レスポンスのパターンおよび所定のレスポンス見積ルールに基づいて前記レスポンスの正当性を見積もるレスポンス見積手段と、前記レスポンス見積手段による見積結果および所定のレスポンス判定ルールに基づいて前記レスポンスを前記クライアントに送信するか否かを判定するレスポンス判定手段と、前記レスポンス判定手段により前記クライアントに送信するものと判定されたレスポンスのみを正当なレスポンスとして前記クライアントに送信するレスポンス送信手段と、をさらに備えたことを特徴とする付記１～１９のいずれか一つに記載のフィルタリング装置。

【０２５９】

（付記２１）前記レスポンス見積手段は、前記レスポンスが前記不正レスポンスデータベースに格納された不正レスポンスのパターンのいずれかに該当する場合に該レスポンスは不正レスポンスである旨を見積もるとともに、前記レスポンスが前記不正レスポンスデータベースに格納された不正レスポンスのパターンのいずれにも該当しない場合に該レスポンスは正当レスポンスである旨を見積もり、

前記レスポンス判定手段は、前記レスポンス見積手段により不正レスポンスである旨が見積もられたレスポンスを前記クライアントに送信しないものと判定するとともに、前記レスポンス見積手段により正当レスポンスである旨が見積もられたレスポンスを前記クライアントに送信するものと判定することを特徴とする付記２０に記載のフィルタリング装置。

【０２６０】

（付記２２）前記レスポンス見積手段は、前記レスポンスが前記不正レスポンスデータベースに格納された不正レスポンスのパターンに該当する度合に応じて所定の見積値を算出し、前記レスポンス判定手段は、前記レスポンス見積手段により算出された見積値と所定の閾値とを比較して前記レスポンスを前記クライアントに送信するか否かを判定することを特徴とする付記２０に記載のフィルタリング装置。

【０２６１】

（付記２３）所定の第３の外部送信ルールに基づいて、前記レスポンス送信手段により前記クライアントに送信されなかったレスポンスおよび／または該レスポンスの起因となったアクセス要求を所定の外部装置に送信する第３の外部送信手段をさらに備えたことを特徴とする付記２０、２１または２２に記載のフィルタリング装置。

【０２６２】

（付記２４）所定の第３の格納ルールに基づいて、前記レスポンス送信手段により前記クライアントに送信されなかったレスポンスおよび／または該レスポンスの起因となったアクセス要求を所定の格納媒体に格納する第３の格納手段をさらに備えたことを特徴とする付記２０～２３のいずれか一つに記載のフィルタリング装置。

【０２６３】

（付記２５）所定の第３の更新ルールに基づいて、前記不正レスポンスデータベース、レスポンス見積ルール、レスポンス判定ルール、第３の外部送信ルール、第３の格納ルールおよび／または第３の更新ルールを更新する第３の更新手段をさらに備えたことを特徴とする付記２０～２４のいずれか一つに記載のフィルタ

リング装置。

【０２６４】

（付記２６）所定の暗号処理がなされたアクセス要求を復号する第１の復号手段をさらに備え、前記第１の見積手段、事前判定手段または第２の見積手段は、前記第１の復号手段により復号されたアクセス要求について見積または判定をおこなうことを特徴とする付記１～２５のいずれか一つに記載のフィルタリング装置。

【０２６５】

（付記２７）前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに受け渡す場合に、前記第１の復号手段により復号されたアクセス要求ではなく、所定の暗号処理がなされたアクセス要求を前記サーバに受け渡すことを特徴とする付記２６に記載のフィルタリング装置。

【０２６６】

（付記２８）所定の暗号処理がなされたレスポンスを復号する第２の復号手段をさらに備え、前記レスポンス見積手段は、前記第２の復号手段により復号されたレスポンスについて見積をおこなうことを特徴とする付記２６または２７に記載のフィルタリング装置。

【０２６７】

（付記２９）前記レスポンスのうちの正当なレスポンスのみを前記クライアントに送信する場合に、前記第２の復号手段により復号されたレスポンスではなく、所定の暗号処理がなされたレスポンスを前記クライアントに送信することを特徴とする付記２８に記載のフィルタリング装置。

【０２６８】

（付記３０）前記サーバに対する不正アクセスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを格納した偽レスポンスデータベースと、前記偽レスポンスデータベースを参照して、不正アクセスとして前記サーバに受け渡されなかったアクセス要求のパターンに対応した偽のレスポンスを作成する偽レスポンス作成手段と、前記偽レスポンス作成手段により作成された偽のレスポンスを前記クライアントに送信する偽レスポンス送信

手段と、をさらに備えたことを特徴とする付記１～２９のいずれか一つに記載のフィルタリング装置。

【０２６９】

（付記３１）不正なアクセスとして前記サーバに受け渡されなかったアクセス要求を受け入れて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを前記サーバのおとりとして作成するおとり手段と、前記おとり手段により作成された偽のレスポンスを前記クライアントに送信する偽レスポンス送信手段と、をさらに備えたことを特徴とする付記１～２９のいずれか一つに記載のフィルタリング装置。

【０２７０】

（付記３２）前記サーバに対する不正アクセスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを格納した偽レスポンスデータベースと、不正アクセスとして前記サーバに受け渡されなかったアクセス要求のうち、前記偽レスポンスデータベースに格納された不正アクセスのパターンに対応するアクセス要求について該パターンに対応した偽のレスポンスを作成する偽レスポンス作成手段と、不正アクセスとして前記サーバに受け渡されなかったアクセス要求のうち、前記偽レスポンスデータベースに格納された不正アクセスのパターンに対応しないアクセス要求を受け入れて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを前記サーバのおとりとして作成するおとり手段と、前記偽レスポンス作成手段または前記おとり手段により作成された偽のレスポンスを前記クライアントに送信する偽レスポンス送信手段と、をさらに備えたことを特徴とする付記１～２９のいずれか一つに記載のフィルタリング装置。

【０２７１】

（付記３３）クライアントと該クライアントからのアクセス要求に応じてサービスを提供するサーバとの間に介在し、前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに受け渡すフィルタリング方法において、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースを参照し、該参照した不正アクセスのパターンおよび所定の第１の見積ルー

ルに基づいて前記アクセス要求の正当性を見積もる第１の見積工程と、

前記第１の見積工程による見積結果および所定の第１の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する第１の判定工程と、

を含んだことを特徴とするフィルタリング方法。

【０２７２】

（付記３４）前記第１の見積工程は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第１の判定工程は、前記第１の見積工程により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記第１の見積工程により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記３３に記載のフィルタリング方法。

【０２７３】

（付記３５）前記第１の見積工程は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、前記第１の判定工程は、前記第１の見積工程により算出された見積値と所定の閾値とを比較して前記アクセス要求を前記サーバに受け渡すか否かを判定することを特徴とする付記３３に記載のフィルタリング方法。

【０２７４】

（付記３６）前記第１の見積工程による正当性の見積もりの前に、前記サーバに対する正当アクセスのパターンを格納した正当パターンデータベースを参照し、前記アクセス要求が前記正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定する事前判定工程をさらに含み、前記第１の見積工程は、前記事前判定工程により正当アクセスのパターンに該当しないものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする付記３３、３４または３５に記載のフィルタリング方法。

【０２７５】

（付記３７）所定の第１の外部送信ルールに基づいて、前記第１の判定工程により前記サーバに受け渡さないものと判定されたアクセス要求を所定の外部装置に送信する第１の外部送信工程をさらに含んだことを特徴とする付記３３～３６のいずれか一つに記載のフィルタリング方法。

【０２７６】

（付記３８）所定の第１の格納ルールに基づいて、前記第１の判定工程により前記サーバに受け渡さないものと判定されたアクセス要求を所定の格納媒体に格納する第１の格納工程をさらに含んだことを特徴とする付記３３～３７のいずれか一つに記載のフィルタリング方法。

【０２７７】

（付記３９）所定の第１の更新ルールに基づいて、前記不正パターンデータベース、正当パターンデータベース、第１の見積ルール、第１の判定ルール、第１の外部送信ルール、第１の格納ルールまたは第１の更新ルールを更新する第１の更新工程をさらに含んだことを特徴とする付記３３～３８のいずれか一つに記載のフィルタリング方法。

【０２７８】

（付記４０）前記サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求に関する情報を格納した統計的不正データベースを参照し、所定の第２の見積ルールに基づいて前記アクセス要求の正当性を見積もる第２の見積工程と、前記見積工程による見積結果および所定の第２の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する第２の判定工程と、前記第１および第２の判定工程により前記サーバに受け渡すものと判定されたアクセス要求のみを正当なアクセス要求として前記サーバに受け渡すアクセス要求受渡工程と、をさらに含んだことを特徴とする付記３３～３９のいずれか一つに記載のフィルタリング方法。

【０２７９】

（付記４１）前記統計的不正データベースは、前記サーバに対してアクセス要求を送信したクライアントのうち、所定時間内のアクセス要求数が所定数を超えた

クライアントの送信元情報を格納するものであって、

前記第２の見積工程は、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第２の判定工程は、前記第２の見積工程により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記第２の見積工程により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記４０に記載のフィルタリング方法。

【０２８０】

（付記４２）前記統計的不正データベースは、前記サーバに対して送信されたアクセス要求の要求内容のうち、所定時間内のアクセス要求数が所定数を超えた要求内容を格納するものであって、

前記第２の見積工程は、前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第２の判定工程は、前記第２の見積工程により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記第２の見積工程により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記４０に記載のフィルタリング方法。

【０２８１】

（付記４３）前記統計的不正データベースは、前記サーバに対してアクセス要求を送信したクライアントのうち、所定時間内のアクセス要求数が所定数を超えたクライアントの送信元情報を格納するとともに、前記サーバに対して送信されたアクセス要求の要求内容のうち、所定時間内のアクセス要求数が所定数を超えた要求内容を格納するものであって、

前記第２の見積工程は、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれかに該当する場合または前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれにも該当しない場合および前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれかにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第２の判定工程は、前記第２の見積工程により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記第２の見積工程により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記４０に記載のフィルタリング方法。

【０２８２】

（付記４４）前記統計的不正データベースは、前記サーバに対してアクセス要求を送信したクライアントのうち、所定時間内のアクセス要求数が所定数を超えたクライアントの送信元情報を格納するとともに、前記サーバに対して送信されたアクセス要求の要求内容のうち、所定時間内のアクセス要求数が所定数を超えた要求内容を格納するものであって、

前記第２の見積工程は、前記アクセス要求の送信元情報および要求内容が前記統計的不正データベースに格納された送信元情報および要求内容に該当する度合に応じて所定の見積値を算出し、前記第２の判定工程は、前記第２の見積工程により算出された見積値と所定の閾値とを比較して前記アクセス要求を前記サーバに受け渡すか否かを判定することを特徴とする付記４０に記載のフィルタリング方法。

【０２８３】

（付記４５）前記第２の見積工程は、前記第１の判定工程により前記サーバに受け渡すものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする付記４０～４４のいずれか一つに記載のフィルタリング方法。

【０２８４】

（付記４６）前記第１の見積工程は、前記第２の判定工程により前記サーバに受け渡すものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする付記４０～４４のいずれか一つに記載のフィルタリング方法。

【０２８５】

（付記４７）前記事前判定工程は、前記第２の判定工程により前記サーバに受け渡すものと判定されたアクセス要求のみについて前記正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定することを特徴とする付記４０～４４のいずれか一つに記載のフィルタリング方法。

【０２８６】

（付記４８）所定の第２の外部送信ルールに基づいて、前記アクセス要求受渡工程により前記サーバに受け渡されなかったアクセス要求を所定の外部装置に送信する第２の外部送信工程をさらに含んだことを特徴とする付記４０～４７のいずれか一つに記載のフィルタリング方法。

【０２８７】

（付記４９）所定の第２の格納ルールに基づいて、前記アクセス要求受渡工程により前記サーバに受け渡されなかったアクセス要求を所定の格納媒体に格納する第２の格納工程をさらに含んだことを特徴とする付記４０～４８のいずれか一つに記載のフィルタリング方法。

【０２８８】

（付記５０）所定の第２の更新ルールおよび／または前記サーバに対するアクセス要求の統計に基づいて、前記統計的不正データベース、第２の見積ルール、第２の判定ルール、第２の外部送信ルール、第２の格納ルールおよび／または第２の更新ルールを更新する第２の更新工程をさらに含んだことを特徴とする付記４０～４９のいずれか一つに記載のフィルタリング方法。

【０２８９】

（付記５１）前記第２の更新工程は、所定時間内に前記サーバに対してアクセス要求を送信した各クライアントごとのアクセス要求数および／または所定時間内に前記サーバに対して送信されたアクセス要求の各要求内容ごとのアクセス要求数に応じて、前記統計的不正データベースに格納される送信元情報および／また

は要求内容を追加および／または削除することを特徴とする付記５０に記載のフィルタリング方法。

【０２９０】

（付記５２）前記アクセス要求に応じて前記サーバから前記クライアントに対して前記サービスとして送信されるレスポンスのうち、前記クライアントに対して送信されるべきでない不正レスポンスのパターンを格納した不正レスポンスデータベースを参照し、所定のレスポンス見積ルールに基づいて前記レスポンスの正当性を見積もるレスポンス見積工程と、前記レスポンス見積工程による見積結果および所定のレスポンス判定ルールに基づいて前記レスポンスを前記クライアントに送信するか否かを判定するレスポンス判定工程と、前記レスポンス判定工程により前記クライアントに送信するものと判定されたレスポンスのみを正当なレスポンスとして前記クライアントに送信するレスポンス送信工程と、をさらに含んだことを特徴とする付記３３～５１のいずれか一つに記載のフィルタリング方法。

【０２９１】

（付記５３）前記レスポンス見積工程は、前記レスポンスが前記不正レスポンスデータベースに格納された不正レスポンスのパターンのいずれかに該当する場合に該レスポンスは不正レスポンスである旨を見積もるとともに、前記レスポンスが前記不正レスポンスデータベースに格納された不正レスポンスのパターンのいずれにも該当しない場合に該レスポンスは正当レスポンスである旨を見積もり、前記レスポンス判定工程は、前記レスポンス見積工程により不正レスポンスである旨が見積もられたレスポンスを前記クライアントに送信しないものと判定するとともに、前記レスポンス見積工程により正当レスポンスである旨が見積もられたレスポンスを前記クライアントに送信するものと判定することを特徴とする付記５２に記載のフィルタリング方法。

【０２９２】

（付記５４）前記レスポンス見積工程は、前記レスポンスが前記不正レスポンスデータベースに格納された不正レスポンスのパターンに該当する度合に応じて所定の見積値を算出し、前記レスポンス判定工程は、前記レスポンス見積工程によ

り算出された見積値と所定の閾値とを比較して前記レスポンスを前記クライアントに送信するか否かを判定することを特徴とする付記５２に記載のフィルタリング方法。

【０２９３】

（付記５５）所定の第３の外部送信ルールに基づいて、前記レスポンス送信工程により前記クライアントに送信されなかったレスポンスおよび／または該レスポンスの起因となったアクセス要求を所定の外部装置に送信する第３の外部送信工程をさらに含んだことを特徴とする付記５２、５３または５４に記載のフィルタリング方法。

【０２９４】

（付記５６）所定の第３の格納ルールに基づいて、前記レスポンス送信工程により前記クライアントに送信されなかったレスポンスおよび／または該レスポンスの起因となったアクセス要求を所定の格納媒体に格納する第３の格納工程をさらに含んだことを特徴とする付記５２～５５のいずれか一つに記載のフィルタリング方法。

【０２９５】

（付記５７）所定の第３の更新ルールに基づいて、前記不正レスポンスデータベース、レスポンス見積ルール、レスポンス判定ルール、第３の外部送信ルール、第３の格納ルールおよび／または第３の更新ルールを更新する第３の更新工程をさらに含んだことを特徴とする付記５２～５６のいずれか一つに記載のフィルタリング方法。

【０２９６】

（付記５８）所定の暗号処理がなされたアクセス要求を復号する第１の復号工程をさらに含み、前記第１の見積工程、事前判定工程または第２の見積工程は、前記第１の復号工程により復号されたアクセス要求について見積または判定をおこなうことを特徴とする付記３３～５７のいずれか一つに記載のフィルタリング方法。

【０２９７】

（付記５９）前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに

受け渡す場合に、前記第１の復号工程により復号されたアクセス要求ではなく、所定の暗号処理がなされたアクセス要求を前記サーバに受け渡すことを特徴とする付記５８に記載のフィルタリング方法。

【０２９８】

（付記６０）所定の暗号処理がなされたレスポンスを復号する第２の復号工程をさらに含み、前記レスポンス見積工程は、前記第２の復号工程により復号されたレスポンスについて見積をおこなうことを特徴とする付記５８または５９に記載のフィルタリング方法。

【０２９９】

（付記６１）前記レスポンスのうちの正当なレスポンスのみを前記クライアントに送信する場合に、前記第２の復号工程により復号されたレスポンスではなく、所定の暗号処理がなされたレスポンスを前記クライアントに送信することを特徴とする付記６０に記載のフィルタリング方法。

【０３００】

（付記６２）前記サーバに対する不正アクセスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを格納した偽レスポンスデータベースを参照して、不正アクセスとして前記サーバに受け渡されなかったアクセス要求のパターンに対応した偽のレスポンスを作成する偽レスポンス作成工程と、前記偽レスポンス作成工程により作成された偽のレスポンスを前記クライアントに送信する偽レスポンス送信工程と、をさらに含んだことを特徴とする付記３３～６１のいずれか一つに記載のフィルタリング方法。

【０３０１】

（付記６３）不正なアクセスとして前記サーバに受け渡されなかったアクセス要求を受け入れて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを前記サーバのおとりとして作成するおとり工程と、前記おとり工程により作成された偽のレスポンスを前記クライアントに送信する偽レスポンス送信工程と、をさらに含んだことを特徴とする付記３３～６１のいずれか一つに記載のフィルタリング方法。

【０３０２】

（付記６４）前記サーバに対する不正アクセスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを格納した偽レスポンスデータベースを参照し、不正アクセスとして前記サーバに受け渡されなかったアクセス要求のうち、前記偽レスポンスデータベースに格納された不正アクセスのパターンに対応するアクセス要求について該パターンに対応した偽のレスポンスを作成する偽レスポンス作成工程と、不正アクセスとして前記サーバに受け渡されなかったアクセス要求のうち、前記偽レスポンスデータベースに格納された不正アクセスのパターンに対応しないアクセス要求を受け入れて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを前記サーバのおとりとして作成するおとり工程と、前記偽レスポンス作成工程または前記おとり工程により作成された偽のレスポンスを前記クライアントに送信する偽レスポンス送信工程と、をさらに含んだことを特徴とする付記３３～６１のいずれか一つに記載のフィルタリング方法。

【０３０３】

（付記６５）前記付記３３～６４のいずれか一つに記載された方法をコンピュータに実行させるプログラム。

【０３０４】

【発明の効果】

以上説明したように、請求項１、８または９の発明によれば、サーバに対する不正アクセスのパターンを格納した不正パターンデータベースの不正アクセスのパターンおよび所定の見積ルールに基づいてアクセス要求の正当性を見積もり、この見積結果および所定の判定ルールに基づいてアクセス要求をサーバに受け渡すか否かを判定することとしたので、アクセス要求の送信元情報ではなくアクセス要求の具体的な要求内容に基づいて不正アクセスであるか否かを判定することができる。これにより、正当なアクセス要求のみをサーバに受け渡すことができ、もって不正クライアントと認定されていないクライアントからの不正アクセスに対してもサーバを防御することができる。

【０３０５】

また、請求項２の発明によれば、アクセス要求が不正パターンデータベースに

格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、アクセス要求が不正パターンデータベースに格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、不正アクセスである旨が見積もられたアクセス要求をサーバに受け渡さないものと判定するとともに、正当アクセスである旨が見積もられたアクセス要求をサーバに受け渡すものと判定することとしたので、アクセス要求が不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを迅速かつ確実に判定することができ、もって不正クライアントと認定されていないクライアントからの不正アクセスに対しても迅速かつ確実にサーバを防御することができる。

【０３０６】

また、請求項３の発明によれば、アクセス要求が不正パターンデータベースに格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、この算出された見積値と所定の閾値とを比較してアクセス要求をサーバに受け渡すか否かを判定することとしたので、見積値および閾値の比較によってある程度の幅を持たせて不正アクセスであるか否かを判定することができ、もって不正クライアントと認定されていないクライアントからの不正アクセスに対してもある程度の幅を持ってサーバを防御することができる。

【０３０７】

また、請求項４の発明によれば、正当性の見積もりの前に、サーバに対する正当アクセスのパターンを格納した正当パターンデータベースを参照し、アクセス要求が正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定し、正当アクセスのパターンに該当しないもの判定されたアクセス要求のみについて正当性を見積もることとしたので、正当アクセスのパターンと一致するアクセス要求については正当性を見積もることなくサーバに受け渡す一方、正当アクセスのパターンと一致しないアクセス要求のみについて正当性を見積もることができ、もって不正アクセスであるか否かを全体としてより迅速に判定することができる。

【０３０８】

また、請求項５の発明によれば、所定の外部送信ルールに基づいて、サーバに受け渡さないものと判定されたアクセス要求を所定の外部装置に送信することとしたので、不正アクセスに関する情報をサーバの管理者、フィルタリング装置の管理者、ネットワーク全般を監視する公的な機関の管理者などに迅速に送信することができ、もってかかる管理者に対しサーバの保全対策を迅速に促すことができる。

【０３０９】

また、請求項６の発明によれば、所定の格納ルールに基づいて、サーバに受け渡さないものと判定されたアクセス要求を所定の格納媒体に格納することとしたので、格納媒体に格納された不正アクセスに関する情報を分析することなどができ、もってサーバの更なる保全対策を講じることができる。

【０３１０】

また、請求項７の発明によれば、所定の更新ルールに基づいて、不正パターンデータベース、正当パターンデータベース、見積ルール、判定ルール、外部送信ルール、格納ルールまたは更新ルールを更新することとしたので、新たに発見された不正アクセスのパターンを不正パターンデータベースに登録することなどができ、もって日々進化する不正アクセスに対して機動的に対応することができる。

【図面の簡単な説明】

【図１】

本実施の形態１に係るサーバクライアントシステムの構成を示すブロック図である。

【図２】

不正リクエストＤＢに格納される情報の構成例を示す図である。

【図３】

本実施の形態１によるフィルタリングの処理手順を説明するフローチャートである。

【図４】

本実施の形態２によるフィルタリングの処理手順を説明するフローチャートで

ある。

【図５】

本実施の形態３に係るサーバクライアントシステムの構成を示すブロック図である。

【図６】

本実施の形態３によるフィルタリングの処理手順を説明するフローチャートである。

【図７】

本実施の形態４に係るサーバクライアントシステムの構成を示すブロック図である。

【図８】

本実施の形態４によるフィルタリングの処理手順を説明するフローチャートである。

【図９】

本実施の形態４の変形例に係るサーバクライアントシステムの構成を示すブロック図である。

【図１０】

本実施の形態５に係るサーバクライアントシステムの構成を示すブロック図である。

【図１１】

本実施の形態６に係るサーバクライアントシステムの構成を示すブロック図である。

【図１２】

本実施の形態６によるフィルタリングの処理手順を説明するフローチャートである。

【図１３】

本実施の形態７に係るサーバクライアントシステムの構成を示すブロック図である。

【図１４】

本実施の形態８に係るサーバクライアントシステムの構成を示すブロック図である。

【図１５】

本実施の形態８によるフィルタリングの処理手順を説明するフローチャートである。

【図１６】

本実施の形態９に係るサーバクライアントシステムの構成を示すブロック図である。

【図１７】

本実施の形態９によるフィルタリングの処理手順を説明するフローチャートである。

【図１８】

本実施の形態１０に係るサーバクライアントシステムの構成を示すブロック図である。

【図１９】

本実施の形態１０に係るサーバクライアントシステムの構成を示すブロック図である。

【符号の説明】

１　ネットワーク

１０　クライアント装置

１１　Ｗｅｂブラウザ

２０、６０　サーバ装置

３０、７０　リクエストフィルタ

３１　受信部

３２　見積部

３２ａ　見積ルール

３３　不正リクエストＤＢ

３４　判定部

３４ａ　判定ルール

３５　送信部

３６　ログ管理部

３６ａ　管理ルール

３７　外部通報部

３７ａ　通報ルール

３８　外部情報取得部

３８ａ　取得ルール

３９　更新部

３９ａ　更新ルール

４０　Ｗｅｂサーバ

５０　外部装置

７１　事前判定部

７１ａ　事前判定ルール

７２　正当リクエストＤＢ

８０、９０　サーバ装置

８１、９１　リクエストフィルタ

８２　第１見積部

８２ａ　見積ルール

８３　不正リクエストＤＢ

８４　第１判定部

８４ａ　判定ルール

８５　第１見積部

８５ａ　見積ルール

８６　統計的不正リクエストＤＢ

８７　第２判定部

８７ａ　判定ルール

８８　送信部

１００　サーバ装置

１０１　リクエストフィルタ

１０２　アクセス管理部

１０３　動的更新部

１０３ａ　更新ルール

１１０、１２０　サーバ装置

１１１、１２１　リクエストフィルタ

１１２　レスポンス受信部

１１３　レスポンス見積部

１１３ａ　見積ルール

１１４　不正レスポンスＤＢ

１１５　レスポンス判定部

１１５ａ　判定ルール

１１６　レスポンス送信部

１２２、１２３　復号部

１３０、１４０、１５０　サーバ装置

１３１、１４１、１５１　リクエストフィルタ

１３２、１５２　偽レスポンス作成部

１３２ａ、１５２ａ　作成ルール

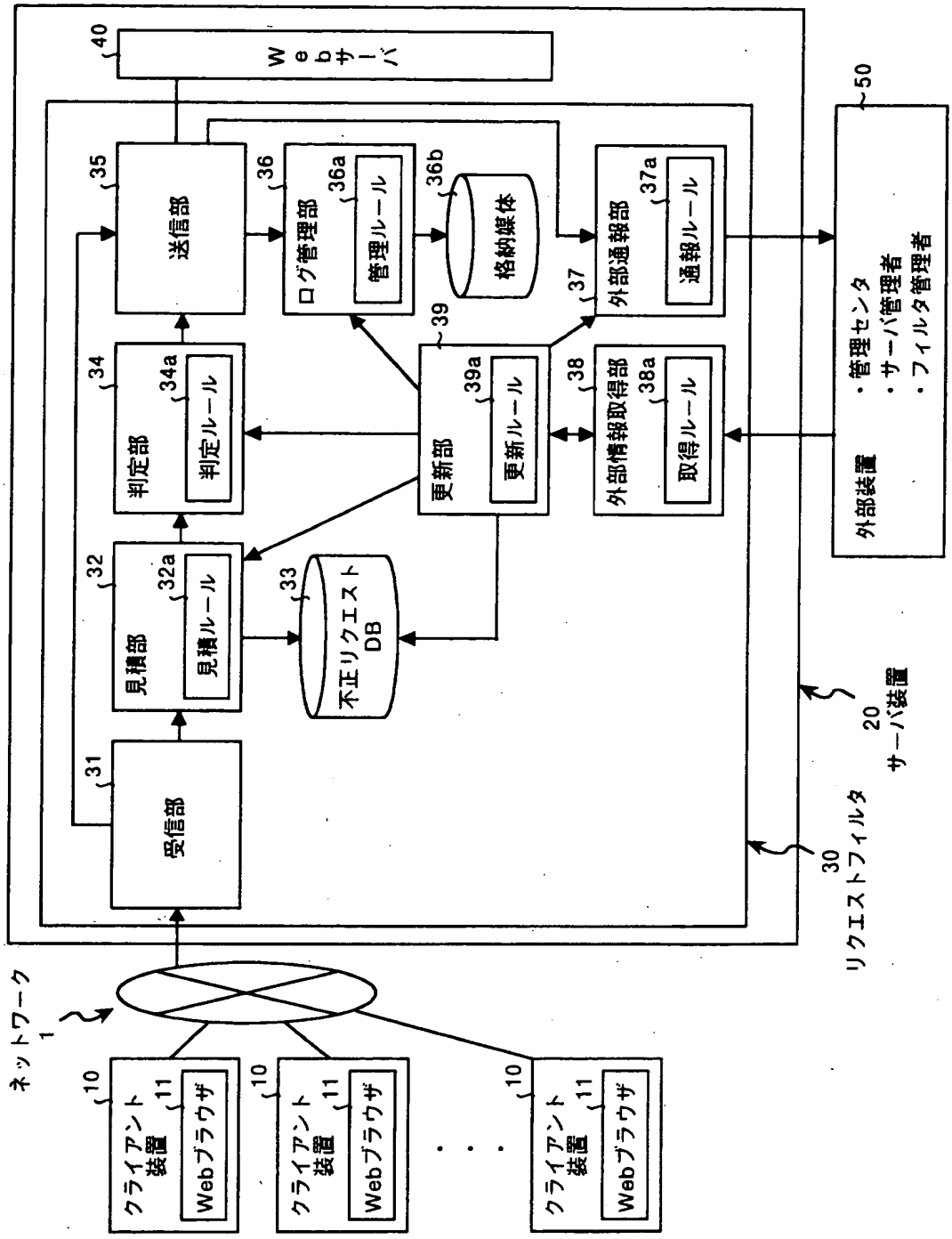
１３３　偽レスポンスＤＢ

１３４　レスポンス送信部

１４２　偽Ｗｅｂサーバ

【書類名】　　図面

【図１】


本実施の形態１に係るサーバクライアントシステムの構成を示すブロック図
ネットワーク
1
クライアント装置
10
Webブラウザ
11
受信部
31
見積部
32
見積ルール
32a
不正リクエストDB
33
判定部
34
判定ルール
34a
送信部
35
ログ管理部
36
管理ルール
36a
格納媒体
36b
外部通報部
37
通報ルール
37a
更新部
39
更新ルール
39a
外部情報取得部
38
取得ルール
38a
Webサーバ
40
リクエストフィルタ
30
サーバ装置
20
外部装置
50
・管理センタ
・サーバ管理者
・フィルタ管理者

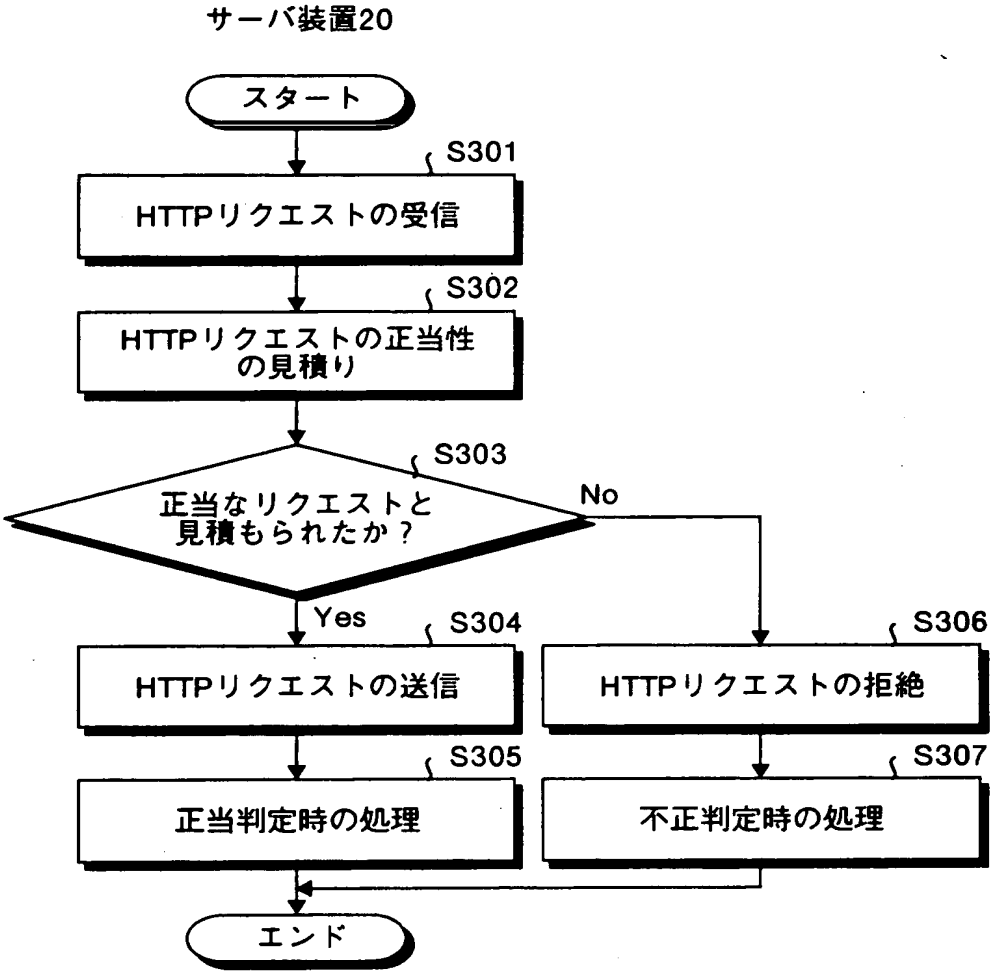
【図２】

不正リクエストDBに格納される情報の構成例を示す図

形式言語パターン	意味
URL=<//	URLの先頭が“//”と一致するリクエストを却下。
CGI==phf ARG=<Qname=root%OA	CGI名が“phf”であり、且つその引数の先頭が“Qname=root%OA”と一致するリクエストを却下。
URL<>..¥..¥..¥..	URLに“..¥..¥..¥..”が含まれるリクエストを却下。
CGI>=.htr	CGI名の末尾が、“.htr”と一致するリクエストを却下。 すなわち、CGIが拡張子“.htr”を有するリクエストを却下。

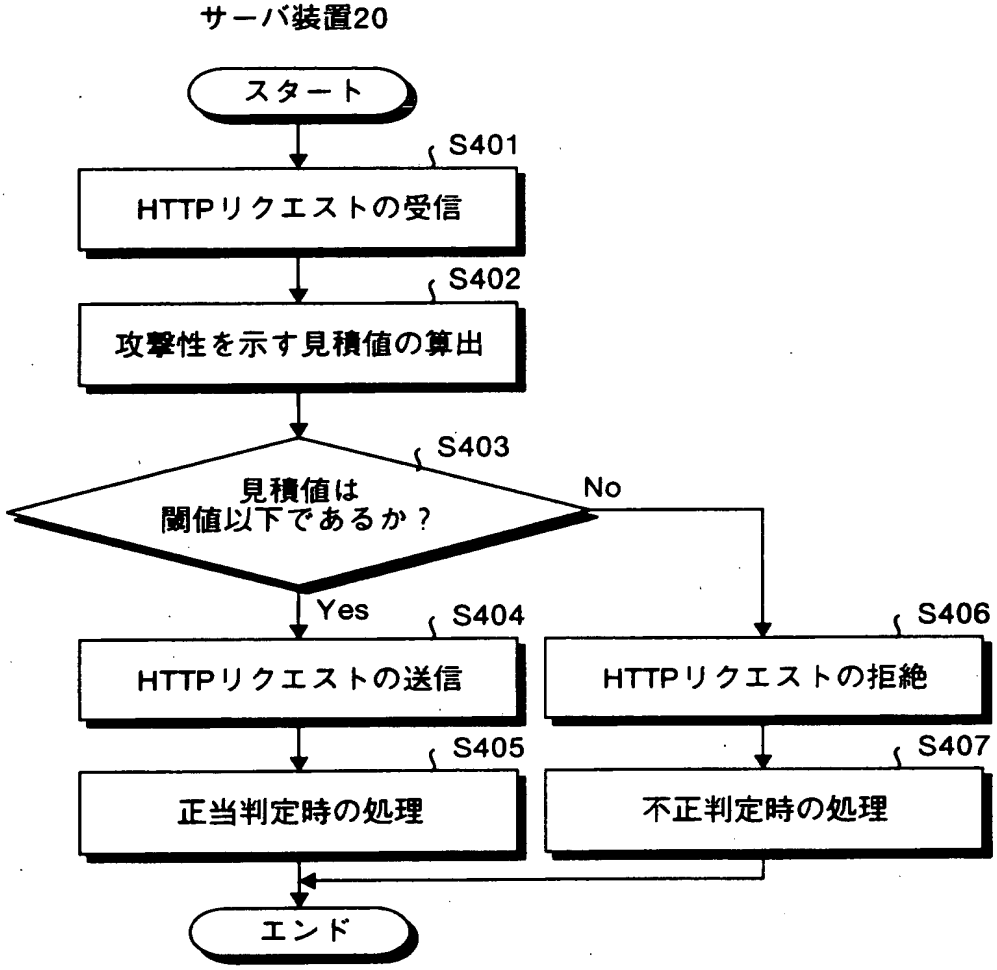
【図３】

本実施の形態１によるフィルタリングの処理手順を示すフローチャート



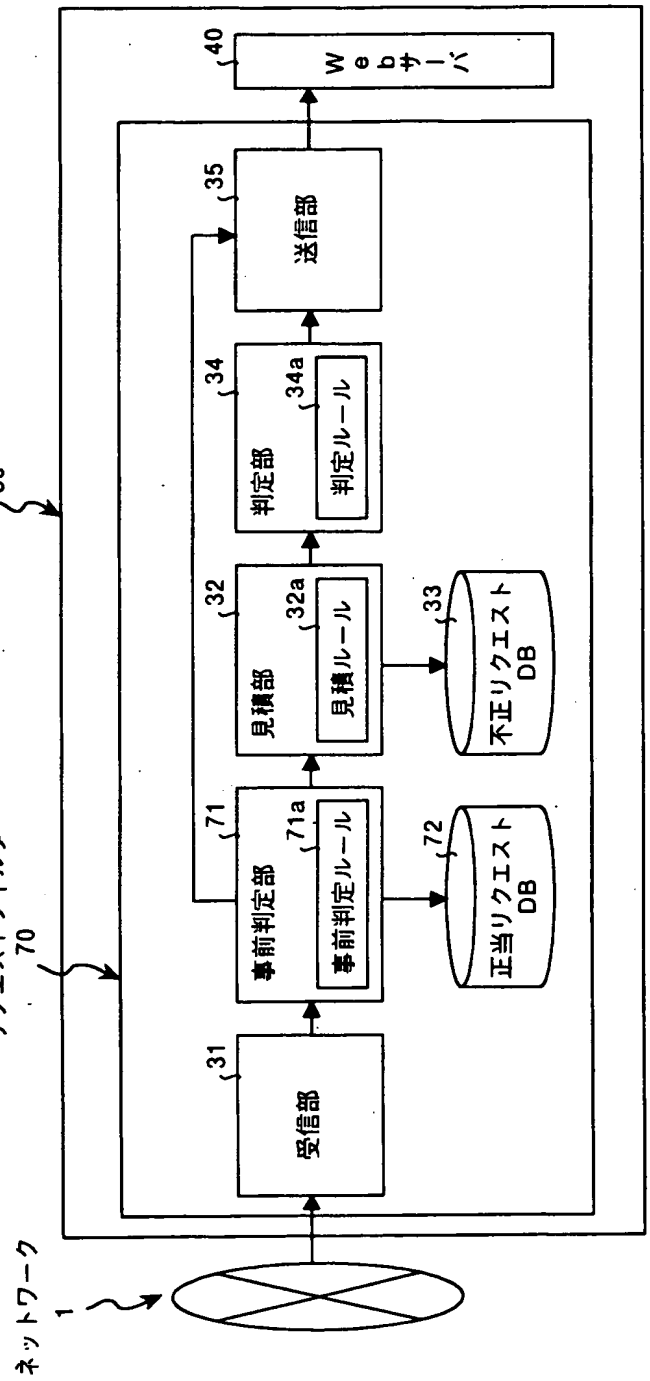
【図４】

本実施の形態２によるフィルタリングの処理手順を示すフローチャート



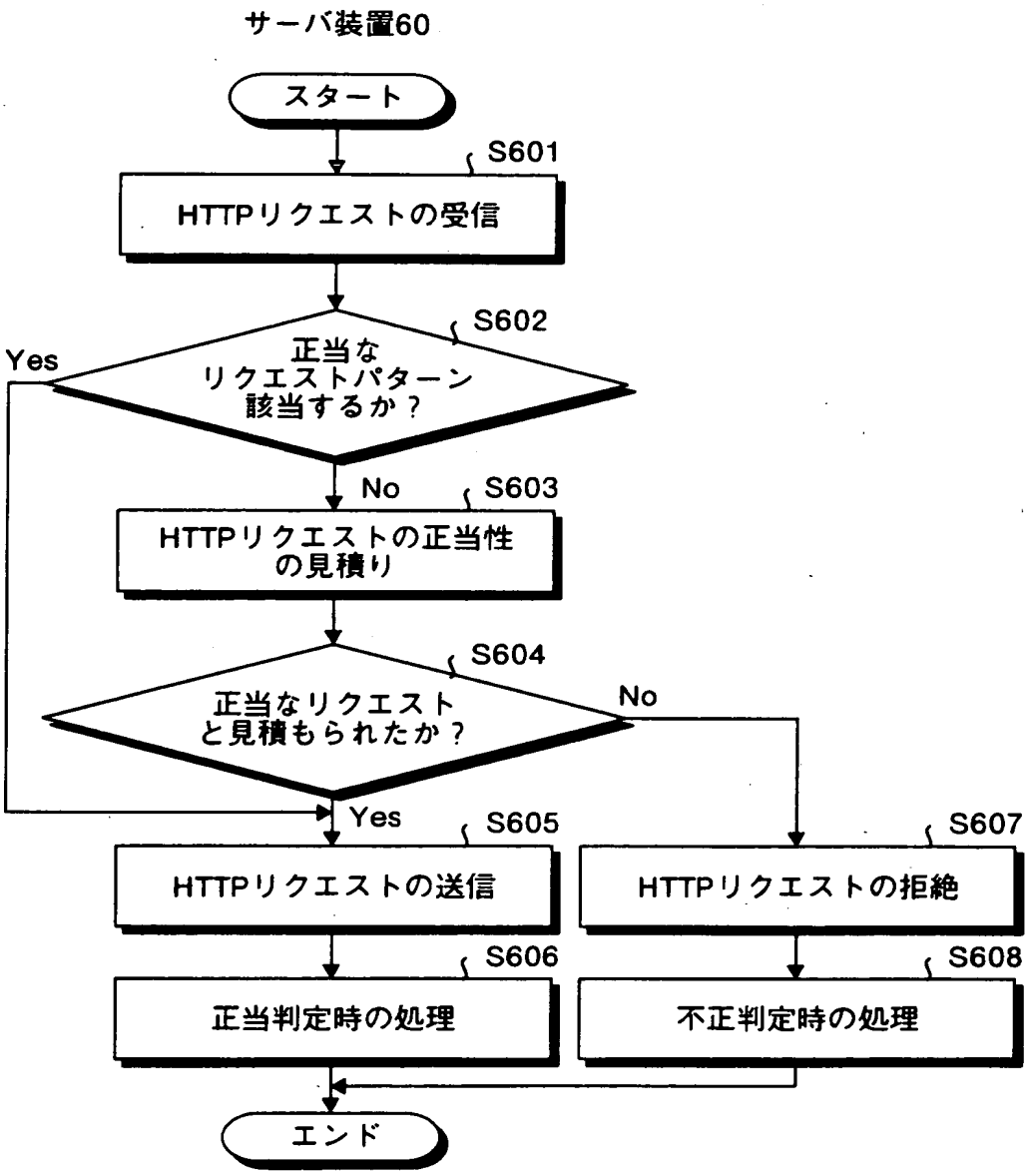
【図５】

本実施の形態３に係るサーバクライアントシステムの構成を示すブロック図

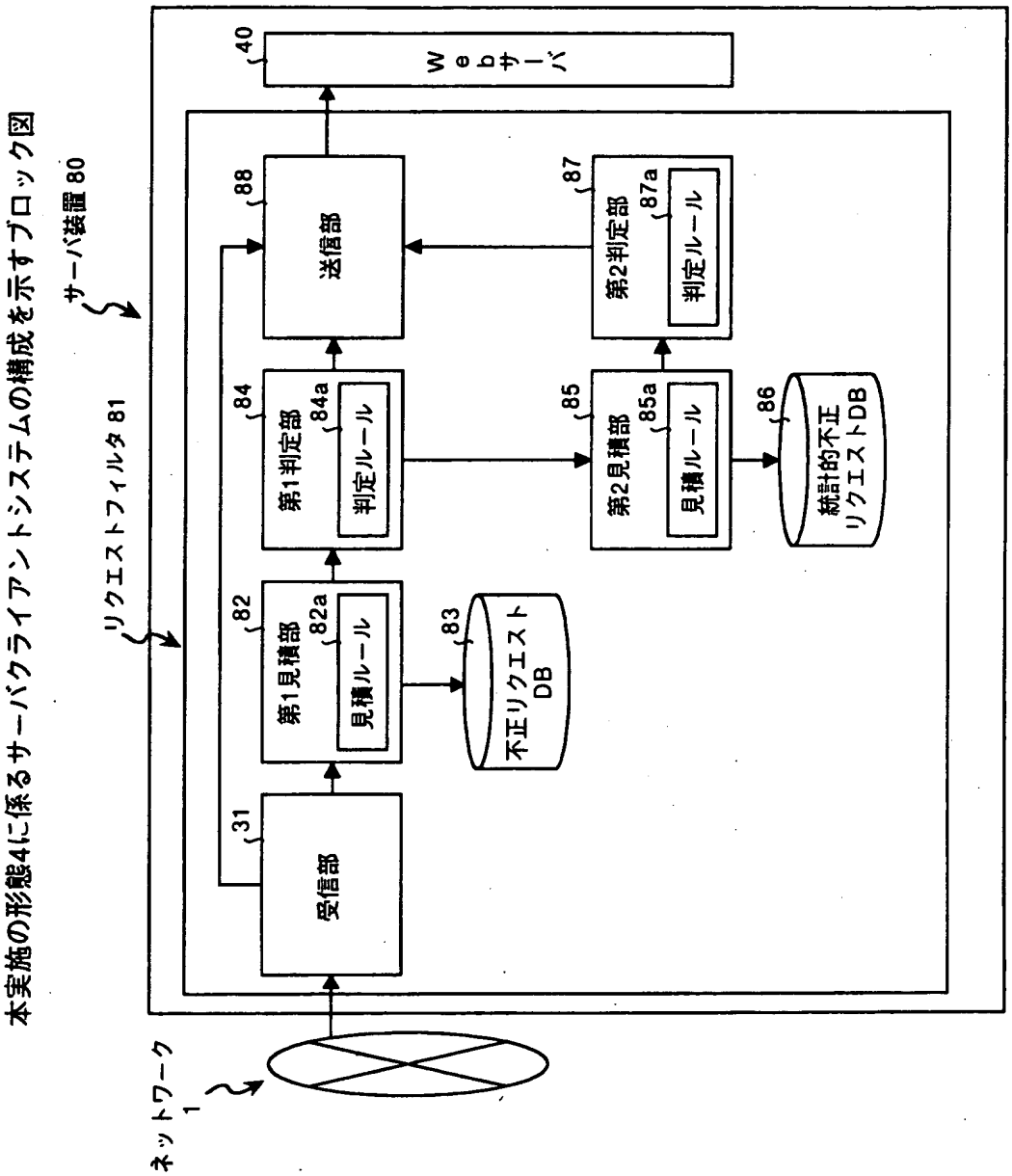


【図６】

本実施の形態３によるフィルタリングの処理手順を示すフローチャート

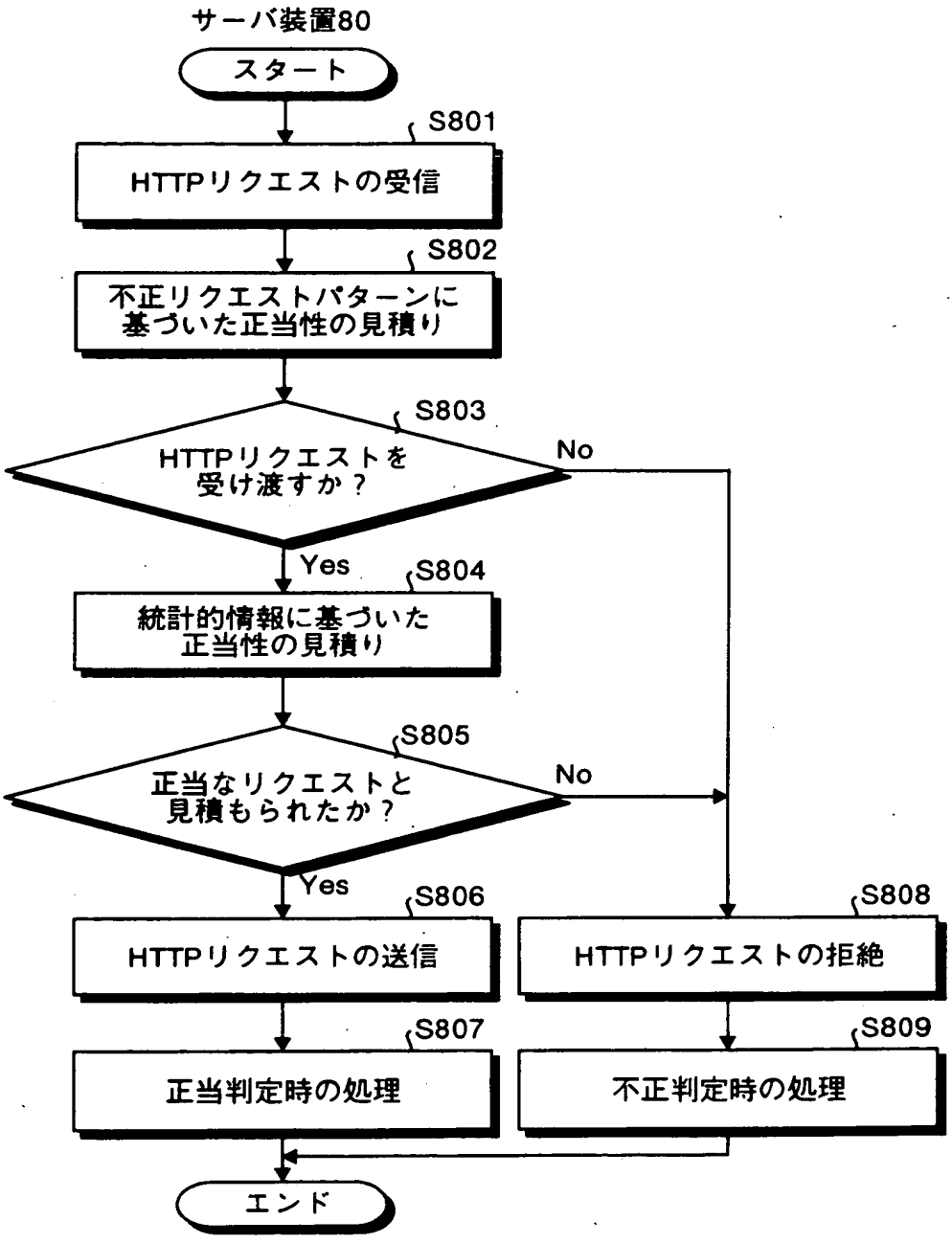


【図７】


本実施の形態4に係るサーバクライアントシステムの構成を示すブロック図
ネットワーク 1
サーバ装置 80
リクエストフィルタ 81
受信部 31
第1見積部 82
見積ルール 82a
不正リクエスト DB 83
第1判定部 84
判定ルール 84a
第2見積部 85
見積ルール 85a
統計的不正リクエストDB 86
第2判定部 87
判定ルール 87a
送信部 88
Webサーバ 40

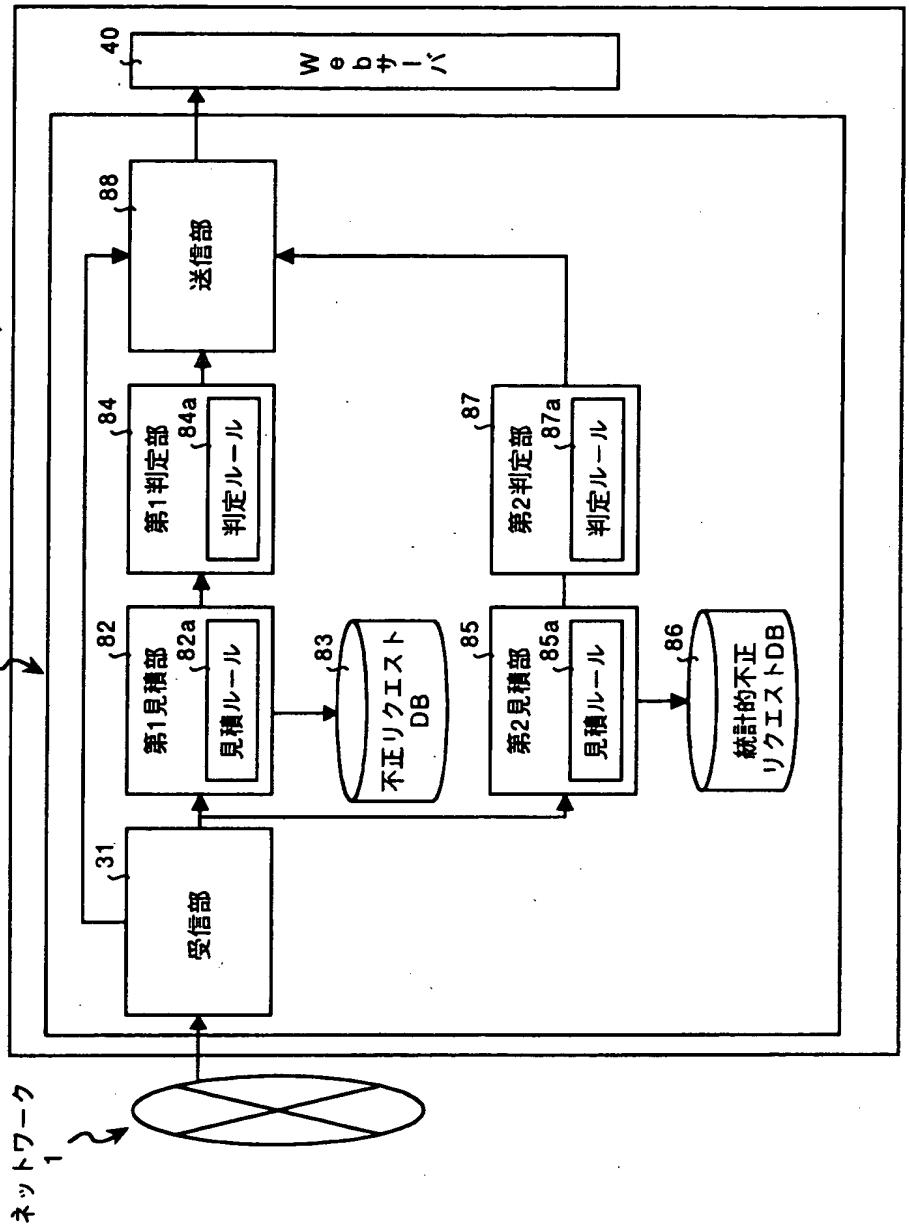
【図８】

本実施の形態4によるフィルタリングの処理手順を示すフローチャート



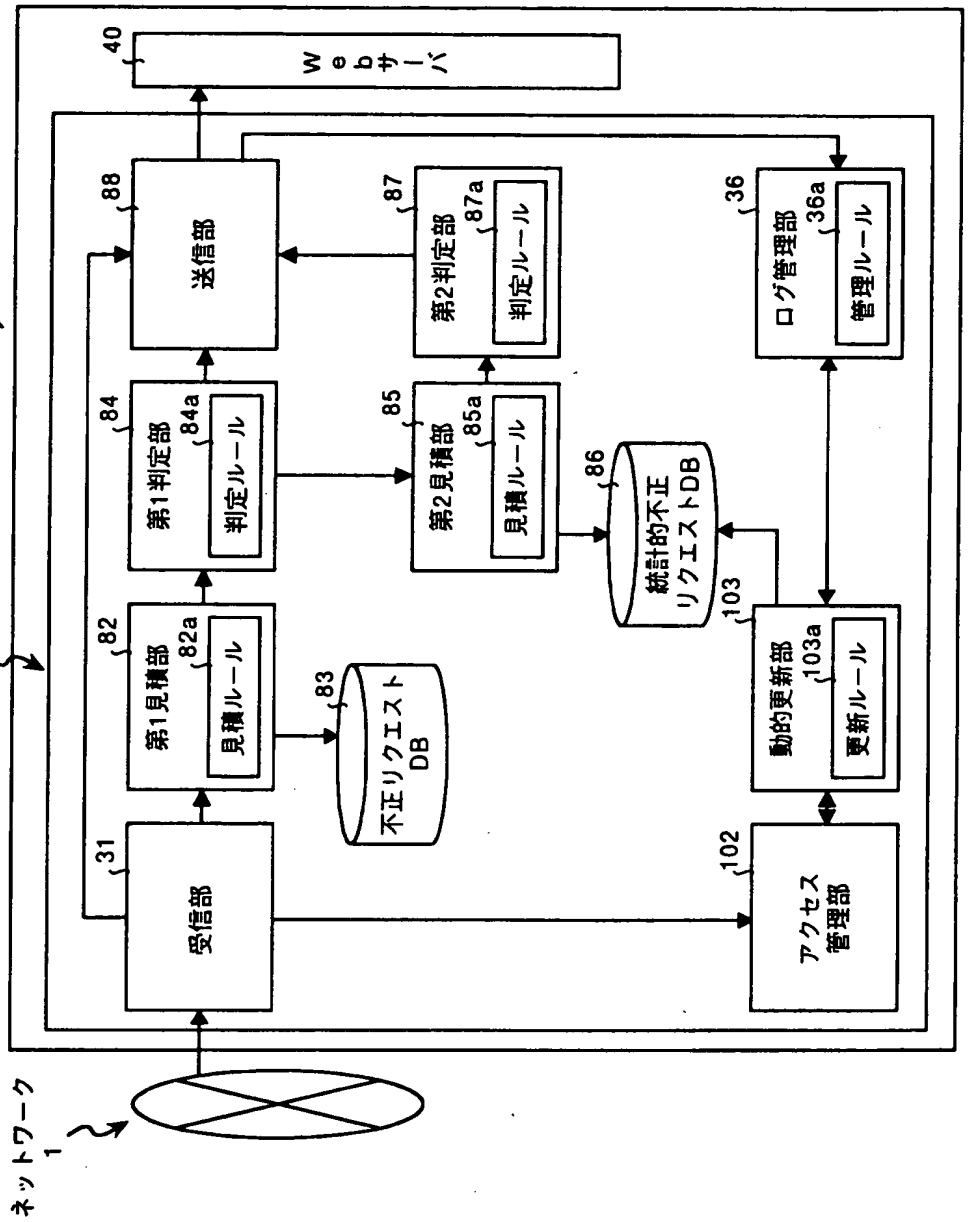
【図９】

本実施の形態4の変形例に係るサーバクライアントシステムの構成を示すブロック図



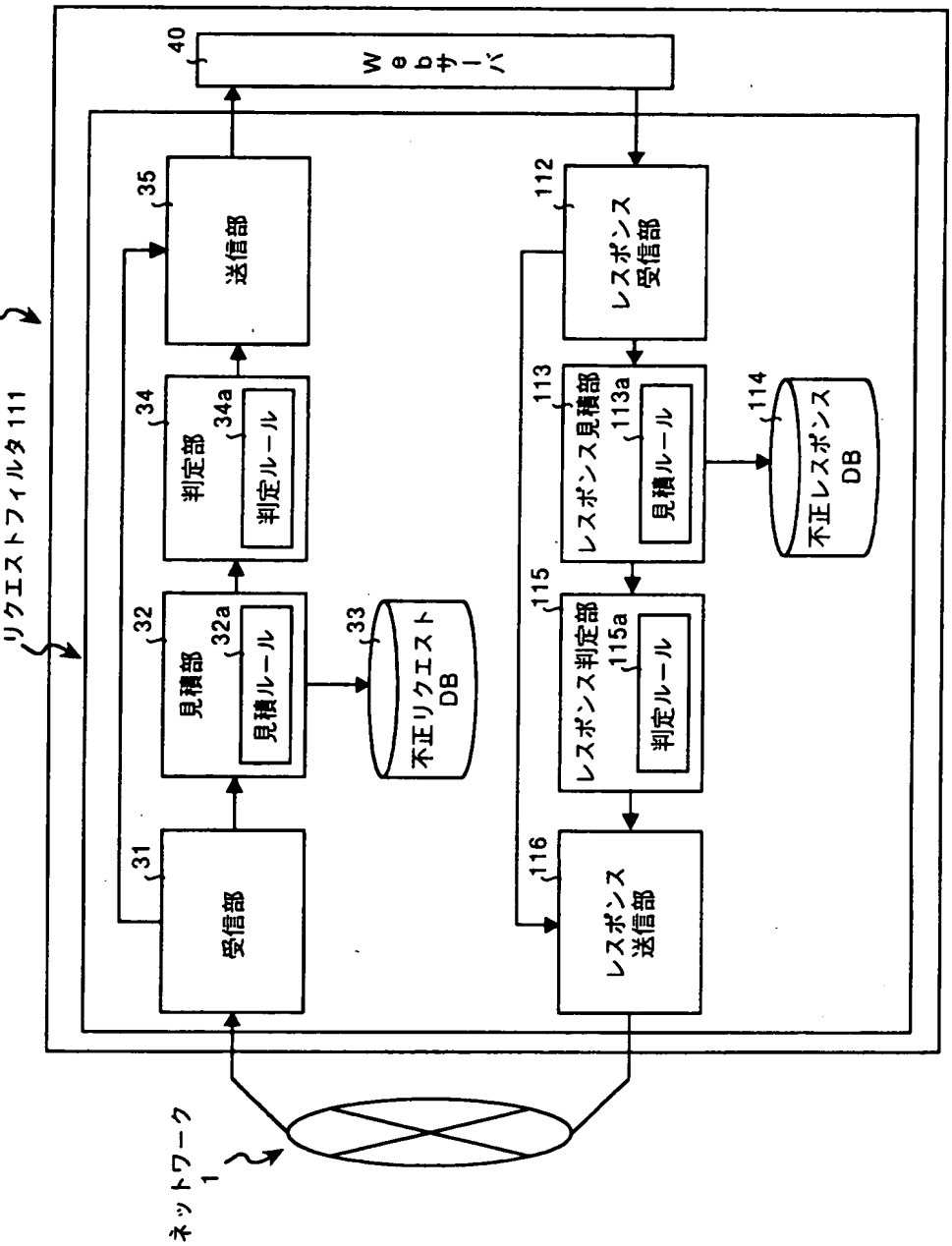
【図１０】

本実施の形態5に係るサーバクライアントシステムの構成を示すブロック図



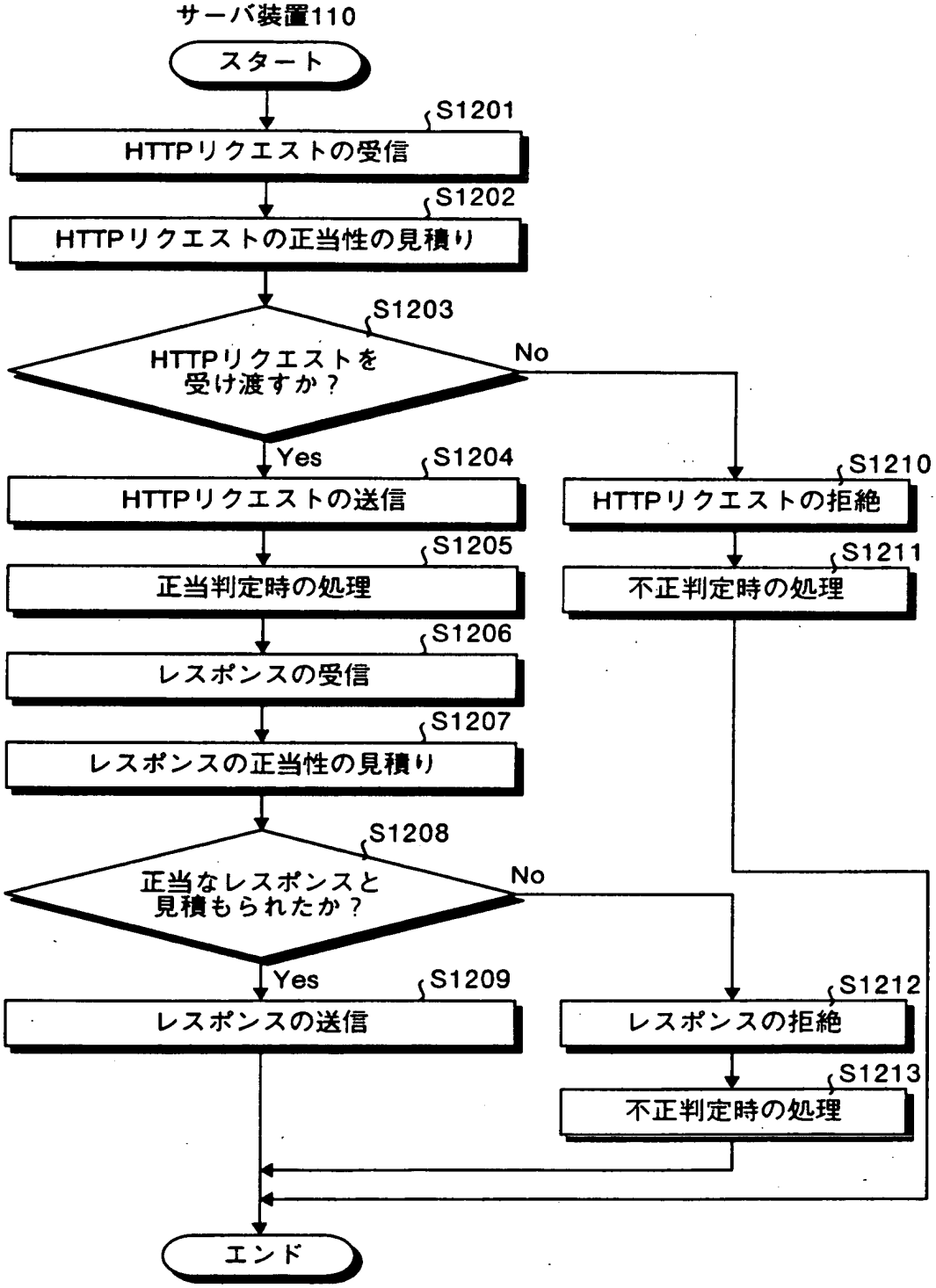
【図１１】

本実施の形態6に係るサーバクライアントシステムの構成を示すブロック図



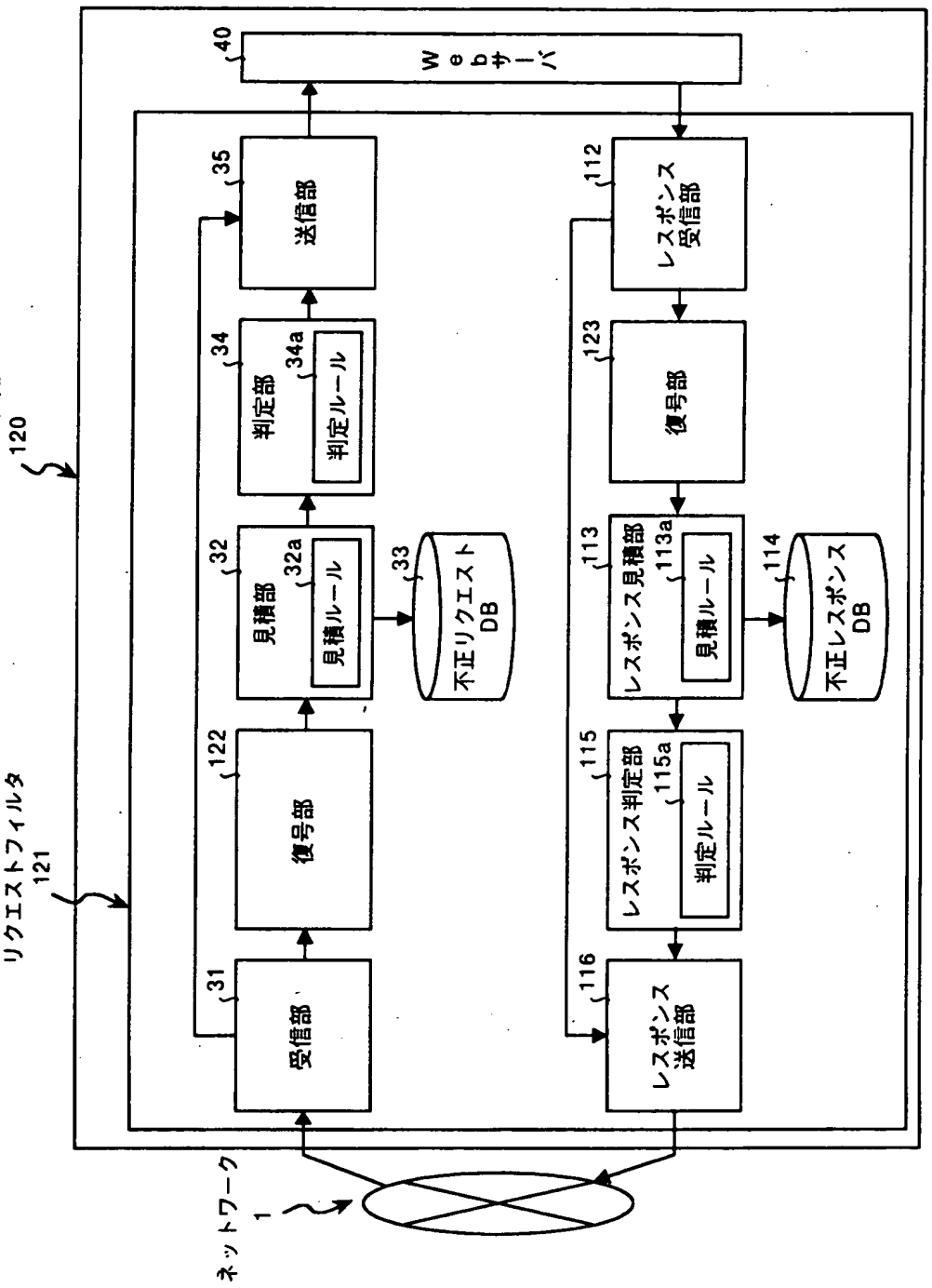
【図１２】

本実施の形態6によるフィルタリングの処理手順を示すフローチャート



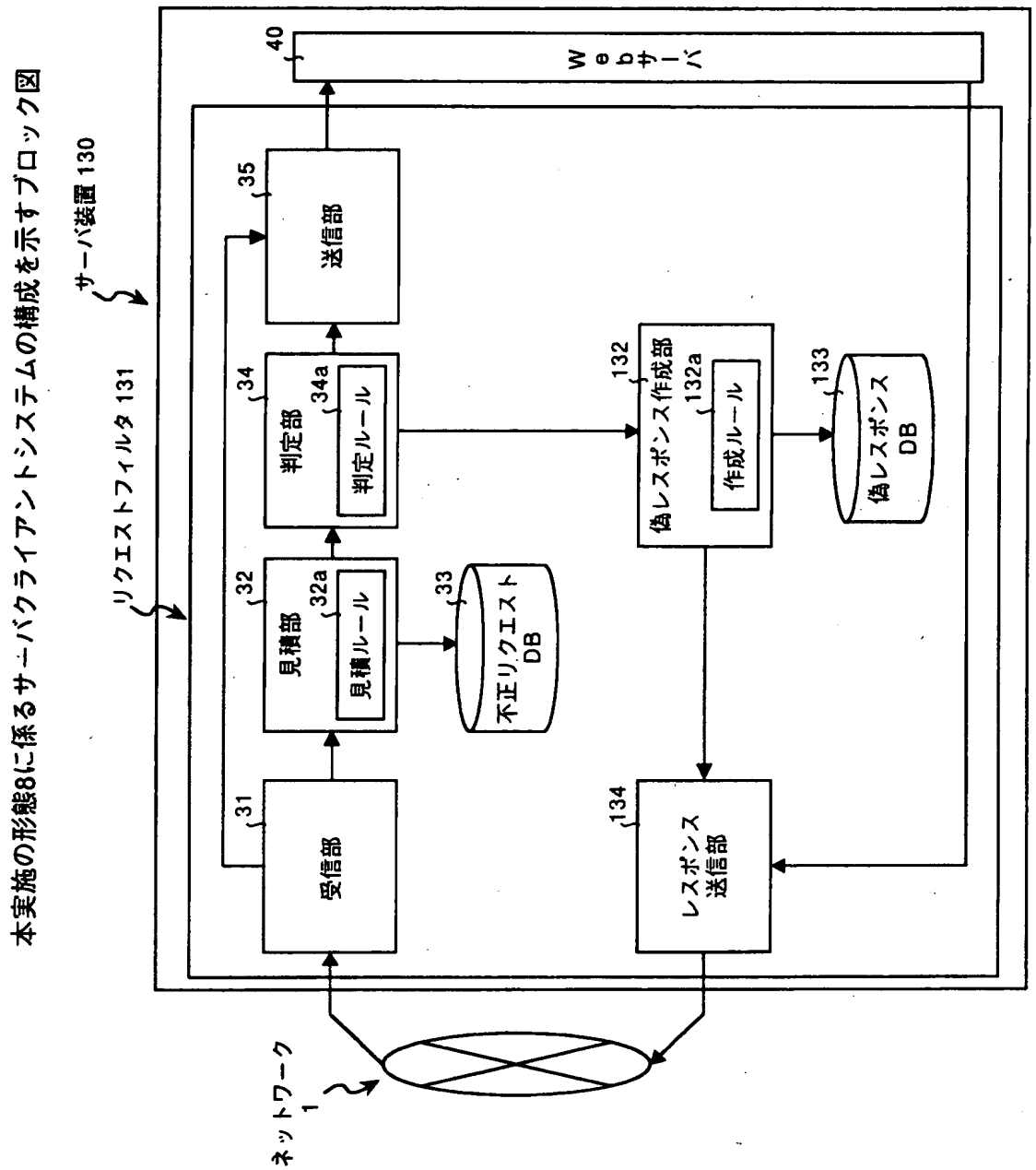
【図１３】

本実施の形態7に係るサーバクライアントシステムの構成を示すブロック図



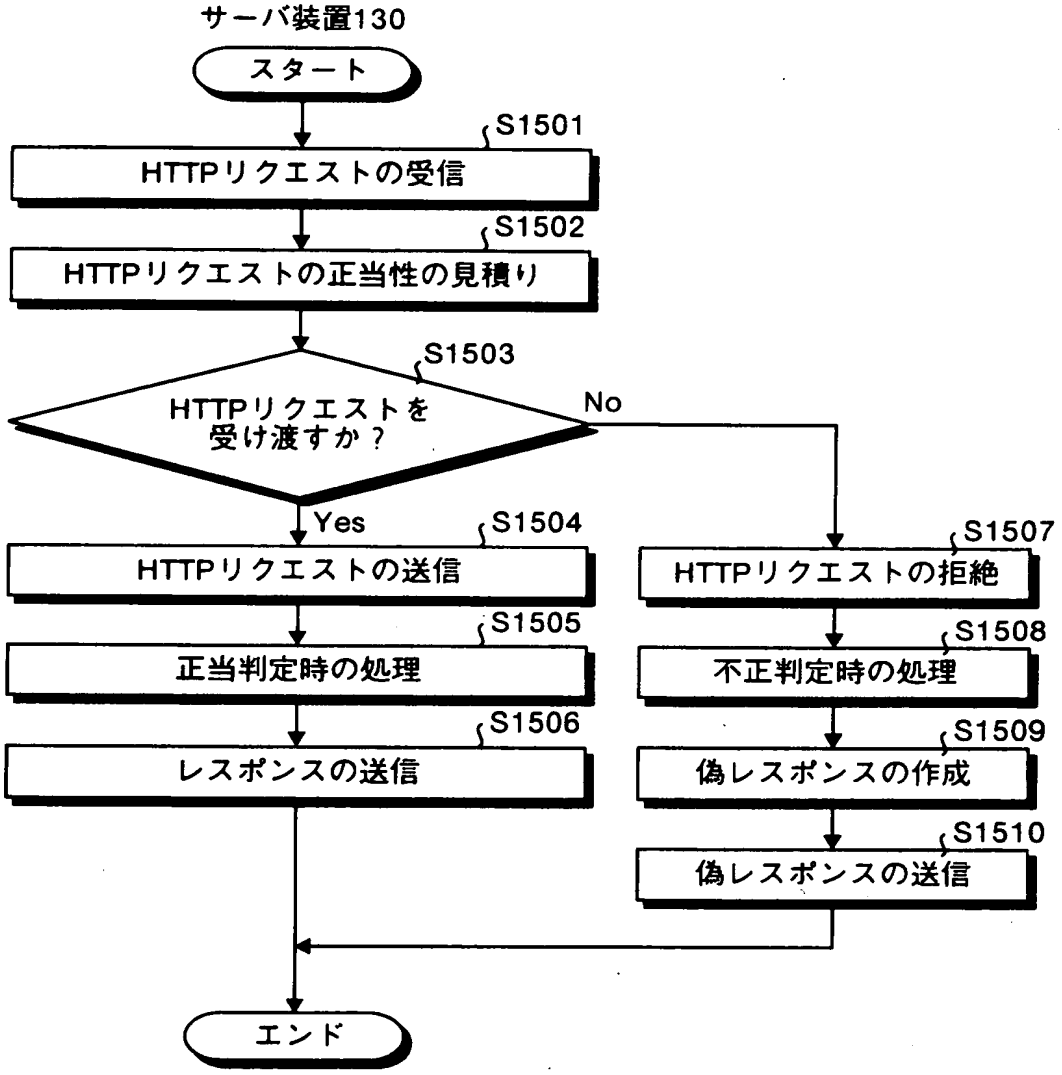
【図１４】

本実施の形態8に係るサーバクライアントシステムの構成を示すブロック図



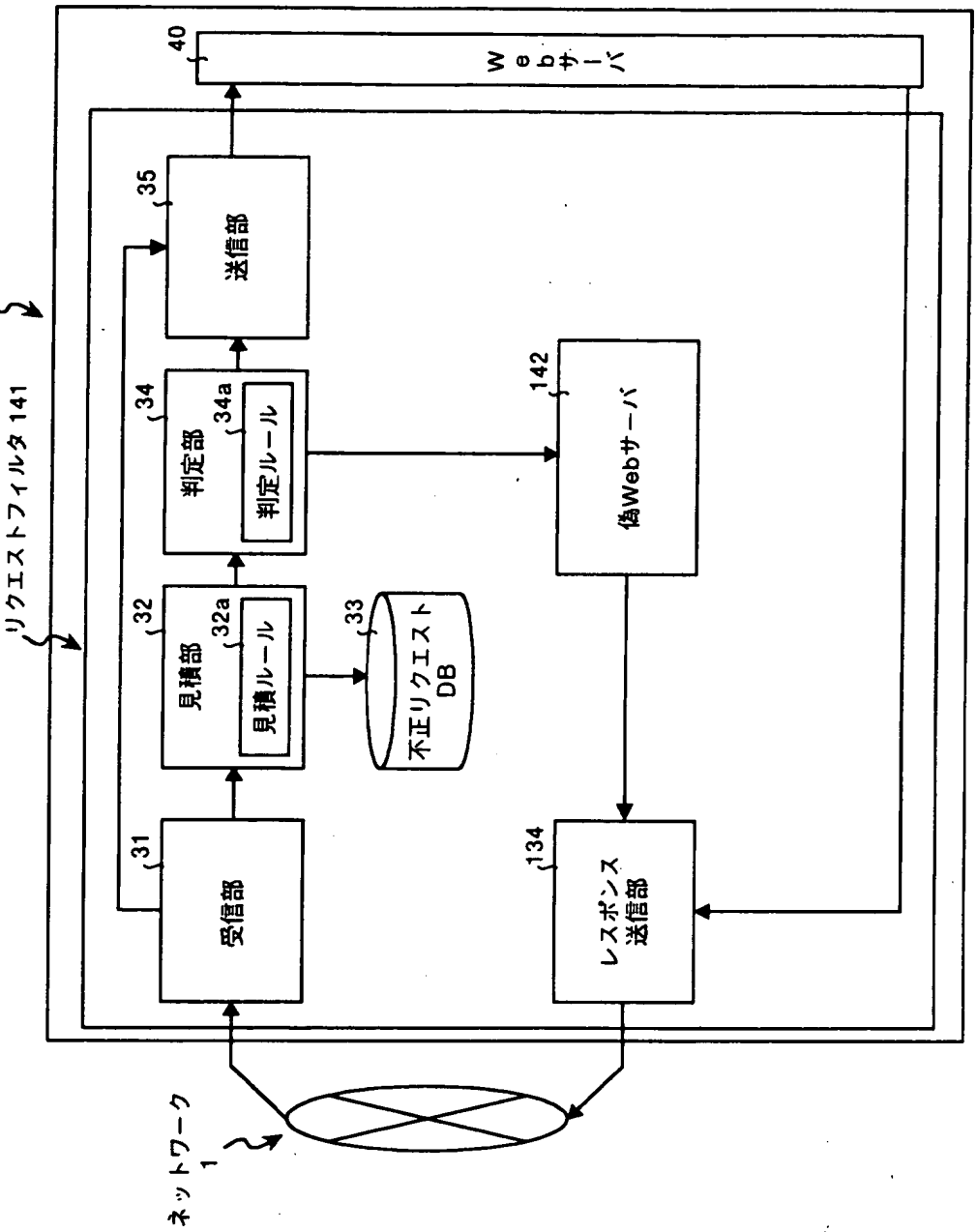
【図１５】

本実施の形態8によるフィルタリングの処理手順を示すフローチャート



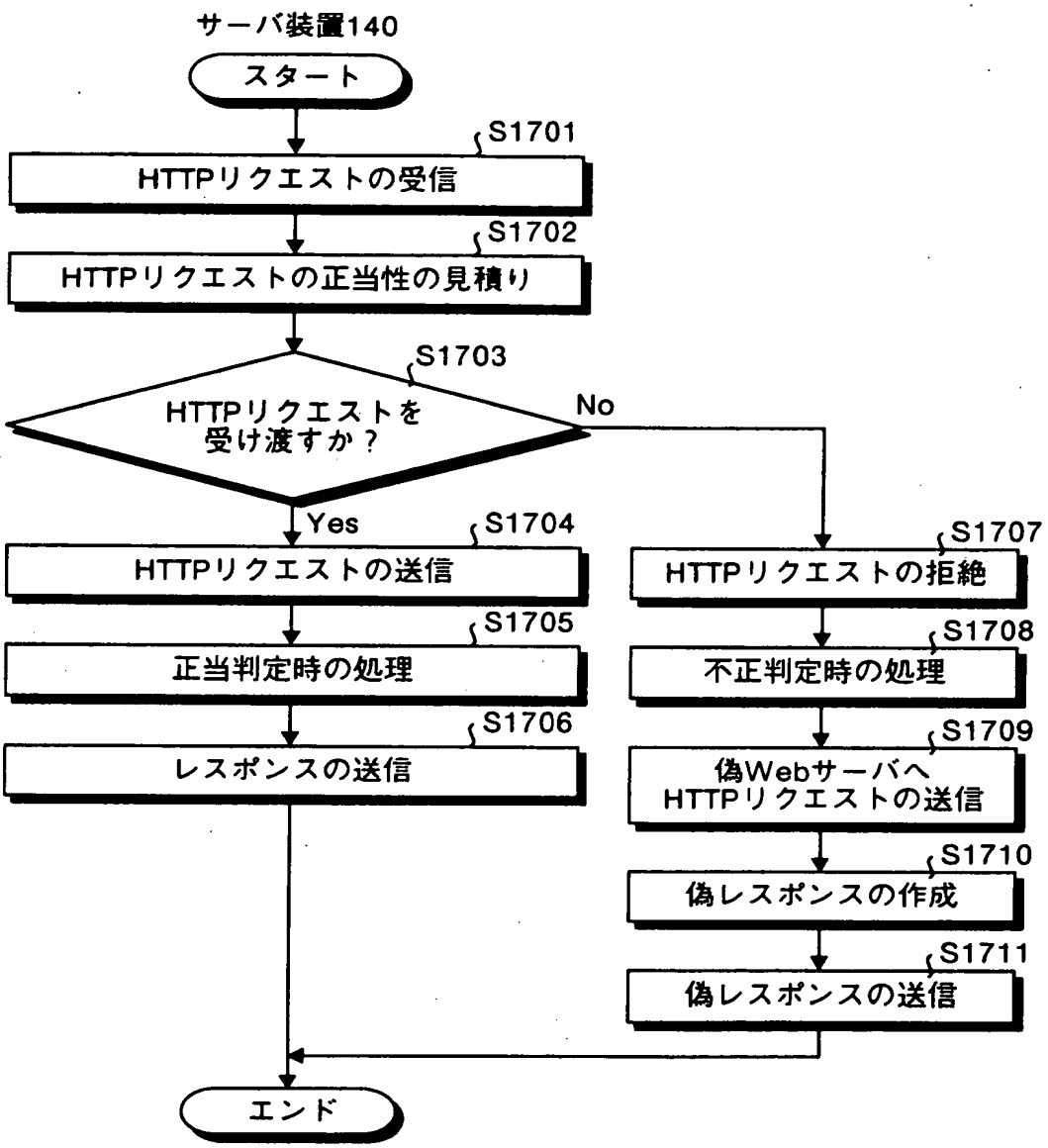
【図１６】

本実施の形態9に係るサーバクライアントシステムの構成を示すブロック図



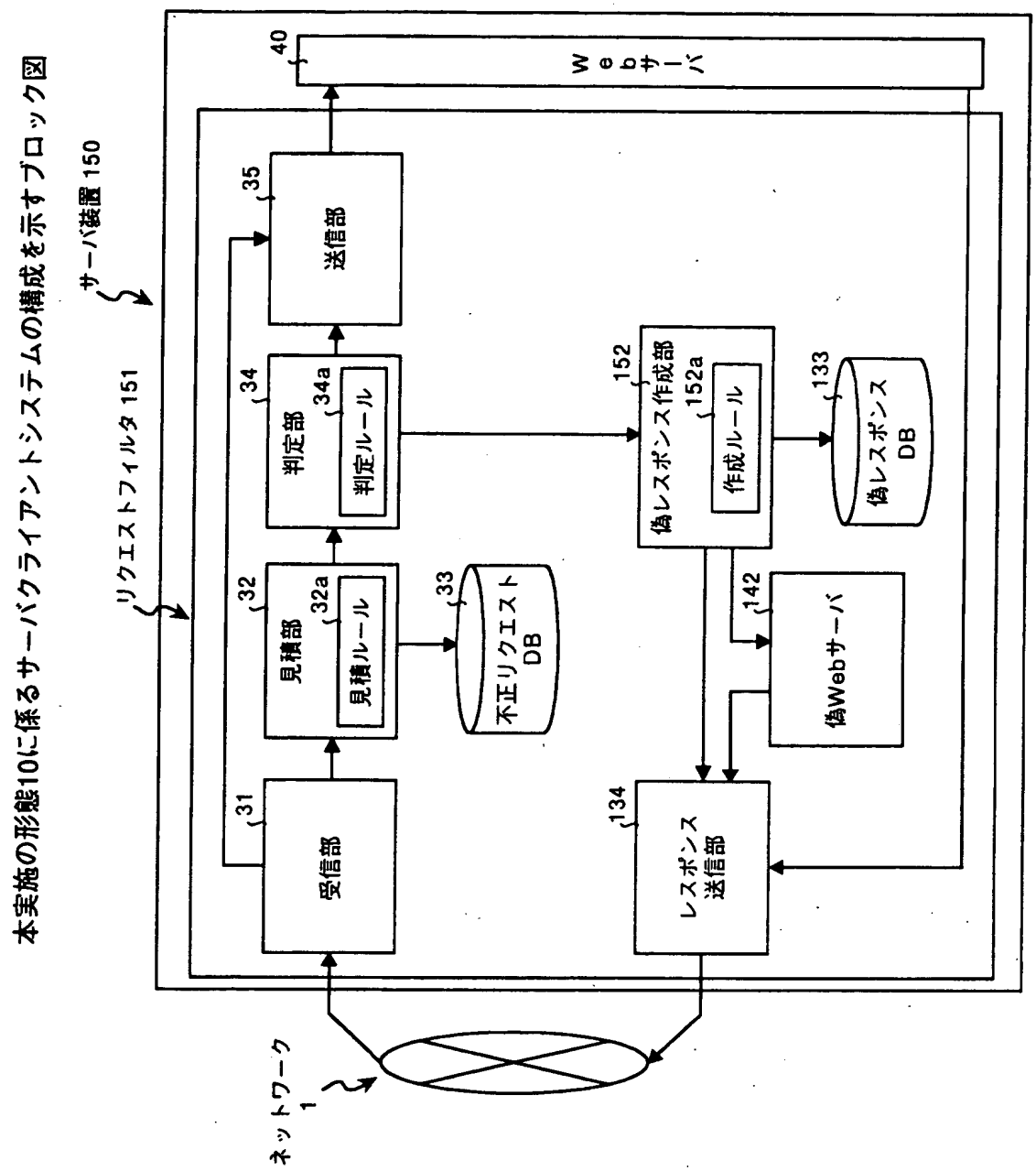
【図１７】

本実施の形態9によるフィルタリングの処理手順を示すフローチャート



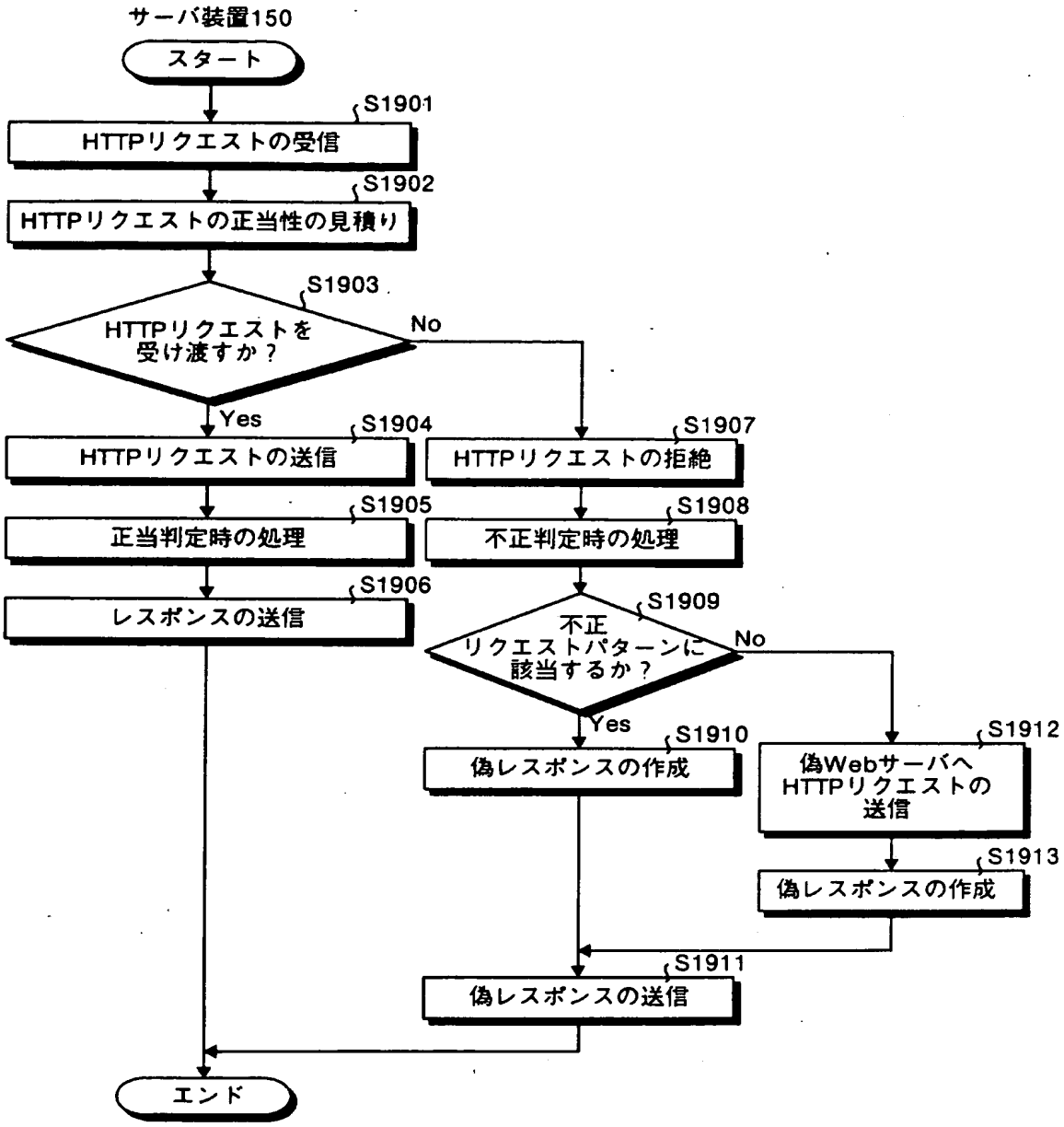
【図１８】

本実施の形態10に係るサーバクライアントシステムの構成を示すブロック図



【図１９】

本実施の形態10によるフィルタリングの処理手順を示すフローチャート



【書類名】　　要約書

【要約】

【課題】　不正クライアントと認定されていないクライアントからの不正アクセスに対してもサーバを防御すること。

【解決手段】　Ｗｅｂサーバ４０に対する不正アクセスのパターンを格納した不正リクエストＤＢ（データベース）３３と、不正リクエストＤＢ３３に格納された不正アクセスのパターンおよび所定の見積ルール３２ａに基づいてクライアント装置１０からのアクセス要求の正当性を見積もる見積部３２と、見積部３２による見積結果および所定の判定ルール３４ａに基づいてアクセス要求をＷｅｂサーバ４０に受け渡すか否かを判定する判定部３４とを備える。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社